An Optimized Content-Aware Authentication Scheme for Streaming JPEG-2000 Images Over Lossy Networks

Zhishou Zhang, *Student Member, IEEE*, Qibin Sun, *Member, IEEE*, Wai-Choong Wong, *Senior Member, IEEE*, John Apostolopoulos, *Senior Member, IEEE*, and Susie Wee, *Senior Member, IEEE*

***Abstract*—This paper proposes an optimized content-aware authentication scheme for JPEG-2000 streams over lossy networks, where a received packet is consumed only when it is both decodable and authenticated. In a JPEG-2000 codestream, some packets are more important than others in terms of coding dependency and image quality. This naturally motivates allocating more redundant authentication information for the more important packets in order to maximize their probability of authentication and thereby minimize the distortion at the receiver. Towards this goal, with the awareness of its corresponding image content, we formulate an optimization framework to compute an authentication graph to maximize the expected media quality at the receiver, given specific authentication overhead and knowledge of network loss rate. System analysis and experimental results demonstrate that the proposed scheme achieves our design goal in that the rate-distortion (R-D) curve of the authenticated image is very close to the R-D curve when no authentication is required.**

***Index Terms*—Content-aware, digital signature, JPEG-2000, signature amortization, stream authentication.**

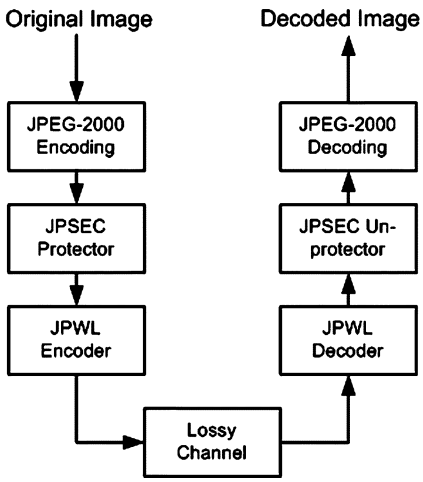

Fig. 1. Scenario where JPSEC and JPWL are working together.

I. Introduction

IT IS becoming increasingly attractive to stream media (e.g., image, audio and video) over today's best-effort network, given the advent of various media coding standards and the rapid growth of network availability and bandwidth. Because of its coding scalability and access flexibility, the latest image-coding standard JPEG-2000 [1], has shown great potential in navigating or streaming very large images such as maps, satellite images, and motion images [2]–[4].

In addition, JPEG-2000 also standardized a network protocol called JPEG-2000 Interactive Protocol (JPIP) [5] and are standardizing the security part called JPSEC [6] and the wireless part called JPWL [7]. JPIP allows interactive and progressive transmission of JPEG-2000 codestreams from server to client. JPSEC defines the framework and tools to address the security issues like access control, encryption, and authentication from stream level to content level [6], [8]–[10]. JPWL provides a set of tools to reduce the undesirable effect caused by network loss. Together, these three parts enable a secure and smooth exchange of JPEG-2000 images over adverse environments, and promote further application of JPEG 2000 standard. Note that if the JPSEC tools are not applied in a manner that accounts for the possibility of packet loss, the packet loss can produce quite adverse effects. Fig. 1 gives an example where a JPEG-2000 codestream is applied with JPSEC authentication tool and JPWL tool before being transmitted. If the loss is not severe, the JPWL tool can still recover the image (although with some distortion), while the JPSEC authentication tool will deem all other packets (which share the same signature or message authentication code with the loss packets) as unauthentic. As it is highly desirable to transmit or stream images over lossy wireless networks like Wi-Fi, 3G and 3.5G, it is desirable to address the security issues over such lossy environments. In this paper, we study the authentication issues for JPEG-2000 image streaming over lossy networks.

Fig. 2 illustrates the typical scenario for image transmission over a lossy channel. At the sender side, the original image is encoded into a stream. In JPEG-2000, the compressed stream is called a *codestream*, which is basically the concatenation of all JPEG-2000 *packets*. Before network transmission, the packets

Manuscript received August 16, 2005; revised June 1, 2006. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Wenjun (Kevin) Zeng.

Z. Zhang is with Institute for Infocomm Research (I2R), Singapore 119613 and also with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117576 (e-mail: zszhang@i2r.a-star.edu.sg).

Q. Sun is with Institute for Infocomm Research (I2R), Singapore 119613. (e-mail: qibin@i2r.a-star.edu.sg).

W.-C. Wong is with Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117576 (e-mail: wong_lawrence@nus.edu.sg).

J. Apostolopoulos and S. Wee are with Hewlett-Packard Laboratories, Palo Alto, CA 94304 USA (e-mail: john_apostolopoulos@hp.com; susie.wee@hp.com).

Digital Object Identifier 10.1109/TMM.2006.886281

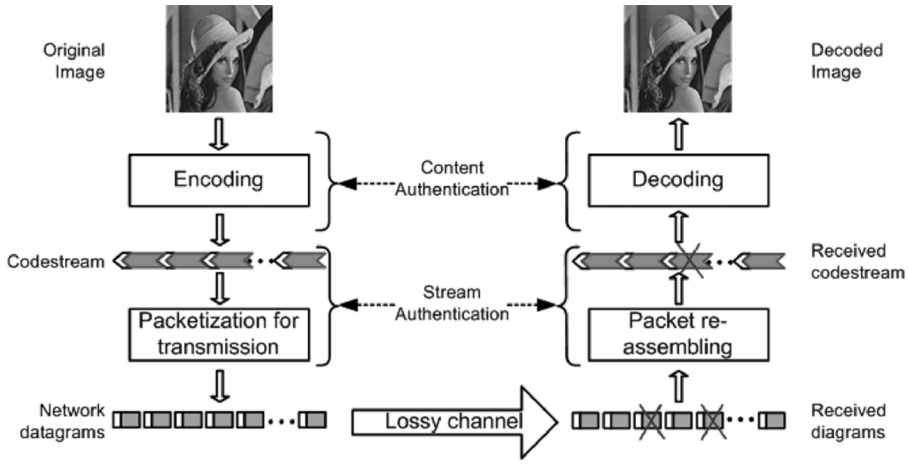

Fig. 2. Image transmission over lossy channel.

have to be segmented into smaller network *datagrams* whose size must be no larger than the *Maximum Transmission Unit (MTU)*. For clarity, we use "*packet* " to denote the JPEG-2000 packet, and use "*datagram* " to denote the basic network transmission unit. At the receiver, the received datagrams are used to assemble the packets. As the channel is lossy, some datagrams may be lost in transit, resulting in corruption of the corresponding packets. Finally, the received packets are decoded to reconstruct the image.

As illustrated in Fig. 2, authentication can be achieved at two different levels: content level and stream level. The authentication at content level, also known as *content authentication* [11], has access to the image content. It is able to extract and sign the key features of the image. Since the extracted features are invariant when the image undergoes content-preserving manipulations, the content authentication is robust against compression and network loss. However, there is a grey area between authentic and unauthentic images. In other words, sometimes it is unable to determine whether the received image is authentic or not. Further, it uses error concealment at the receiver site which may not be feasible for some computation-limited applications such as cell phones because the state-of-the-art error concealment operations are still very time and computation consuming.

The authentication at stream level, also known as *stream authentication*, has access to the stream packets only. Existing stream authentication schemes [12]–[16], some of which can resist packet loss to a certain degree, amortize one signature among a group of packets that are connected via a directed acyclic graph. To increase the verification probability, the hash of a packet is appended to several other packets. Since the stream authentication does not utilize content information, it has to assume all packets are equally important and tries to increase the verification probability for every packet, which results in high overhead. Because stream authentication applies one-way hash and signature directly on the packets, the verification results have no ambiguity (i.e., either authentic or unauthentic) and still maintain the same security as traditional digital signature schemes such as DSA or RSA [17].

In this paper, we propose an optimized content-aware stream authentication scheme for various media streams over lossy networks. In the subsequent sections, we are only concerned with JPEG-2000 streams. By utilizing the image content information which is usually extracted during image encoding, the proposed scheme minimizes the expected distortion of the authenticated image at the receiver while still maintaining an acceptable level of communication overhead and a high verification probability. The basic idea is, each packet is associated with a quantity ΔD, which is the amount by which the overall distortion will be reduced if the packet is consumed. The quantity ΔD could be directly derived from the distortion field in JPSEC [6] and JPWL [7]. For more important packets (i.e., with larger ΔD), to increase their verification probability we replicate and append their hashes in greater numbers to other packets, which increase their verification probability as well as the overhead. Conversely, less important packets can have lower verification probability and lower overhead. Therefore, with the content information available, we formulate an optimization framework to compute an authentication graph to maximize the expected media quality at the receiver, given specific authentication overhead and knowledge of network loss rate. To differentiate from other existing stream authentication schemes which are all focusing on maximizing the verification probability, we therefore name the proposed solution as content-aware stream authentication scheme. In addition, the proposed solution is compliant with JPEG-2000, JPWL and JPSEC, because it works at the packet level and thereby does not change the packet format. In other words, it can take packets generated by a JPEG-2000 encoder, JPWL encoder or JPSEC encoder, and constructs an authentication graph before transmission over lossy network.

This paper is organized as follows. Section II describes related works in the area of stream authentication, and gives some preliminary information about JPEG-2000. Section III presents the proposed distortion-overhead optimization framework for media authentication. The proposed content-aware authentication scheme for JPEG-2000 streams is presented in Section IV, followed by the system analysis in Section V. Experimental results are presented in Section VI. Finally, Section VII concludes this paper.

II. Background

A. Prior Work on Stream Authentication

Wong and Lam [12] proposed a stream authentication scheme based on the Merkle authentication tree [18], where the leaf

node is the packet hash and the internal node is the hash of their child nodes. Only the root node is signed. However, each packet has to carry the signature, its position in the tree and the sibling of each node along its path to the root. Although each packet is individually verifiable, the communication overhead is terribly high which is not feasible for media streaming.

Gennaro and Rohatgi [13] proposed a simple hash chain to authenticate a block of packets using only one signature. Each packet is appended with the hash of the next packet, and only the first packet is signed. This scheme has very low overhead (only 1 hash/packet), but it is not robust against loss. Any packet loss will break the hash chain, and subsequent packets are not verifiable.

Perrig *et al.* [14] proposed the efficient multichannel stream signature (EMSS), which extended the idea of Gennaro and Rohatgi [13]. To achieve robustness against packet loss, the hash of a packet is appended to several other subsequent packets that are randomly selected, and the final signature packet signs on the hashes of multiple packets.

Golle and Modadugu [15] proposed a scheme called augmented chains. Recognizing that packet loss is usually bursty, the augmented chain is designed with two types of hash links: global links and local links. The global links, whose source and target are further away in the sequence, are used to resist against burst loss. The local links are mainly used to link all packets into the augment chains.

The butterfly authentication scheme [16] connects the packet via a butterfly graph. Due to the good fault-tolerance of the butterfly graph, this scheme has improved verification probability compared with the other schemes under the same overhead level.

All the above-mentioned schemes have a common problem, i.e., they only take into account the network loss model and assume all packets are equally important. Furthermore, robustness is measured by the verification probability only. However, for a media stream, in many cases it is more appropriate to measure robustness by the reconstructed media quality. Having the content information available, we can differentiate the packets by assigning the more important packets with more authentication overhead and thereby higher verification probability, and vice versa. Therefore, we are able to design a more efficient stream authentication scheme that can maximize the quality of the authenticated image for a given overhead, or can minimize the overhead to achieve a desired authenticated image quality.

B. JPEG-2000 Basics

JPEG-2000 employs discrete wavelet transform (DWT) to transform an image into *resolutions* and *sub-bands*, followed by *quantization*. The quantized coefficients are then arranged into *codeblocks*. Fig. 3 illustrates how an image of 256 $\times$ 256 pixels is decomposed into three resolutions and each subband consists of codeblocks of 64 $\times$ 64 coefficients.

The quantized coefficients are coded in two tiers. In Tier-1 coding, each codeblock is encoded independently. The coefficients are bit-plane encoded, starting from the most significant bit-plane all the way to the least significant one. Furthermore, all bit-planes except the most significant one are split into three sub-bit-plane passes (coding passes), where the information that

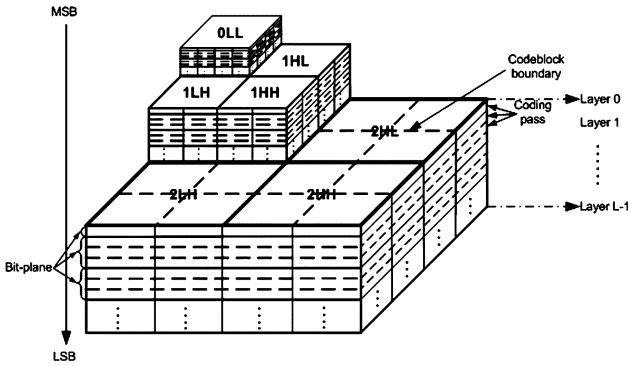

Fig. 3. JPEG-2000 resolutions, subbands, codeblocks, bit-planes, and coding passes.

results in largest reduction in distortion will be encoded first. We denote a coding pass of codeblock B_i by $C_i^{(p,k)}$ where p indicates the bit-plane (bit-plane 0 is the least significant bit-plane) and k denotes the coding pass within a bit-plane ($k = 1$, 2, or 3). Each coding pass results in a sequence of codewords, whose length is denoted by $l_i^{(p,k)}$. The amount of distortion reduction of coding pass $C_i^{(p,k)}$ of codeblock B_i can be calculated as (1). The distortion is measured in the square-error unit

$$\Delta d_i^{(p,k)} = G_{b_i} \sum_{j \in C_i^{(p,k)}} ((\hat{y}^{p+1}[j] - y[j])^2 - (\hat{y}^{p}[j] - y[j])^2). \tag{1}$$

In (1), G_{b_i} is the energy gain factor for the subband, where codeblock B_i is located, $y[j]$ is the value of the jth coefficient in B_i, and $\hat{y}^p[j]$ is the reconstructed value when the jth coefficient is decoded up to bit-plane p. For more details, refer to [19] and [20].

Tier-2 coding introduces another three structures: *layers*, *precincts* and *packets*. The *layers* enable quality scalability, and each *layer* includes a number of consecutive coding passes contributed by individual codeblocks. The *precinct* is a collection of spatially contiguous codeblocks from all sub-bands at a particular resolution. All the coding passes that belong to a particular precinct P_m and a particular layer L_l constitute a *packet*, denoted by P_m^l. Assuming an additive distortion model, the amount of distortion reduction for a packet P_m^l can be calculated by summing up the distortion reductions of all the coding passes that constitute this packet, as

$$\Delta D_m^l = \sum_{B_i \in P_m} \sum_{C_i^{(p,k)} \in L_l} \Delta d_i^{(p,k)}. \tag{2}$$

Similarly, the length of packet P_m^l can be calculated by summing up the lengths of all the coding passes and the packet header R_{hdr}, as:

$$R_m^l = R_{\mathrm{hdr}} + \sum_{B_i \in P_m} \sum_{C_i^{(p,k)} \in L_l} l_i^{(p,k)}. \tag{2}$$

In order to illustrate the distribution of packets' importance, we encode the "bike" image [shown in Fig. 8(c)] with 16 layers and 80 packets per layer, and compute the distortion reduction for every individual packet, which are depicted in Fig. 4.

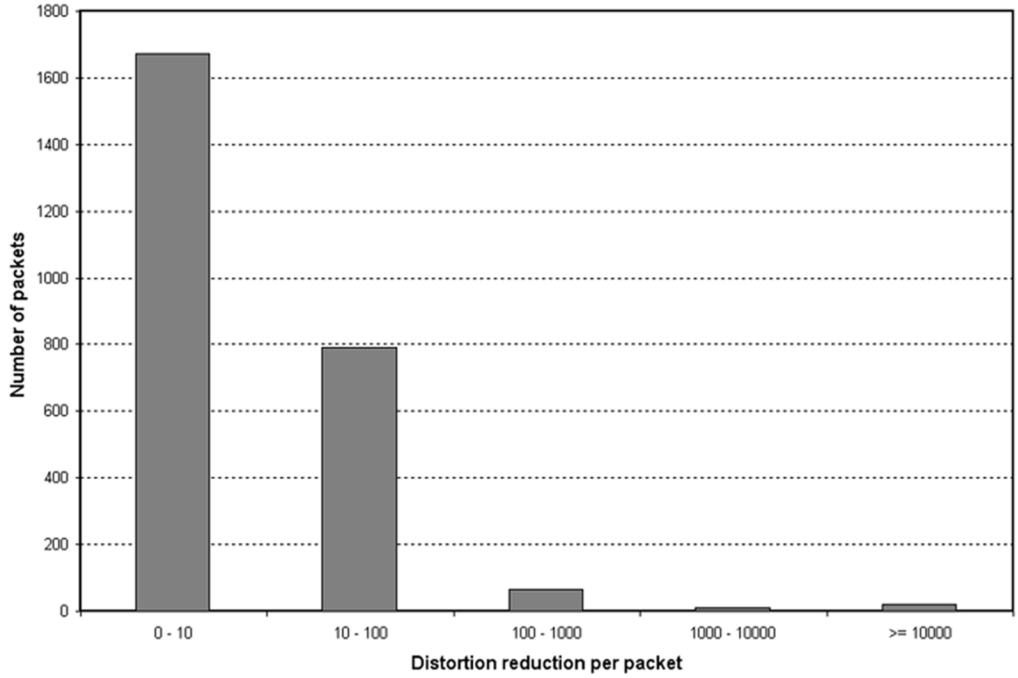

Fig. 4. Distribution of packets' distortion reduction in a JPEG-2000 codestream.

The amount of distortion reduction per packet exhibits huge differences. Out of the 2560 packets, 2464 packets (more than 96%) have a distortion reduction less than 100 MSE units, and the other 96 packets (less than 4%) have much greater distortion reduction. In other words, a small number of packets are much more important than the rest of the packets. This characteristic is often exploited via unequal error protection to transport the media data over lossy networks. Similarly, stream authentication can also utilize this characteristic by increasing the redundancy degree for more important packets, so as to increase their verification probability, and vice versa to greatly reduce overhead without compromising reconstructed visual quality.

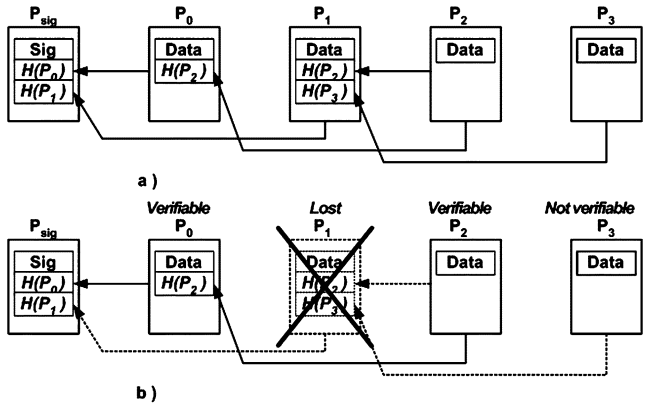

Fig. 5. Authentication graph at the sender and receiver. (a) Authentication graph at the sender. (b) Authentication graph at the receiver

III. Distortion-Overhead Optimization Framework for Media Authentication

The problem of authenticating an image stream can be solved in the distortion-overhead Optimization framework, which can used to construct an authentication graph trading off two conflicting goals: minimal authentication overhead and minimal distortion (or maximal media quality) of the authenticated image. Given a specific overhead level and network condition, we try to compute an authentication graph that minimizes the distortion of the authenticated image. Conversely, the optimized graph minimizes the authentication overhead, given a specific distortion and network condition. In other words, the distortion-overhead performance of the optimized authentication graph lies on the lower convex hull of the set of all achievable distortion-overhead performances.

An authentication graph is a directed acyclic graph denoted by $\langle V, G \rangle$, where V is the set of nodes and G is the set of directed edges in the graph. A *node* in V corresponds to a *JPEG-2000 packet* or a *signature packet* signed with a crypto signature scheme, and there is typically only one signature packet in V. A *directed edge* $e(i,j)$ from node P_i to P_j indicates that the hash value of P_i is appended to P_j, where P_i and P_j are referred to as the *source node* (or *source packet*) and *target node* (or *target packet*), respectively. The edge $e(i,j)$ is also referred to as a *hash link* that connects P_i to P_j. The *redundancy degree* of the packet P_i is the number of edges coming out of P_i. In particular, the redundancy degree is 0 for a signature packet. At the receiver, the nodes corresponding to the lost packets are removed from the graph. A packet P_i is *verifiable* if there remains a path from P_i to the signature packet. The *verification probability* is the probability that a packet is verifiable given that it is received. Fig. 5(a) gives an example of an authentication graph constructed at the sender side and Fig. 5(b) gives the remaining graph after the packet P_1 is lost in transit.

To formulate the distortion-overhead optimization problem, we define the vector variable $\pi = [\pi_0, \pi_1, \ldots, \pi_m, \ldots, \pi_{M-1}]$, where π_m is the set of target nodes of the edges coming out of P_m The redundancy degree of P_m is $|\pi_m|$, where $|\pi_m| \geq 1$. Obviously, given the set of nodes V, the variable π uniquely defines

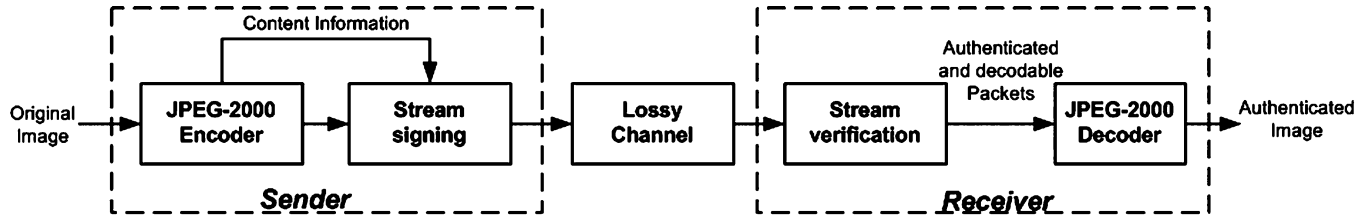

Fig. 6. Content-aware authentication system over lossy network.

the authentication graph. Denoting the total authentication overhead (i.e., signature and hashes) as O and the overall expected distortion as D, our goal is to find the optimal variable π^* that minimizes the expected Lagrangian in (4) for a given $\lambda > 0$. The Lagrange multiplier λ is used to control the trade-off between the overhead O and the expected distortion D. For instance, a smaller value of λ will result in an optimized policy leading to smaller expected distortion D and higher overhead O, and vice versa

$$\pi^* = \arg\min_{\pi}(D + \lambda O). \tag{4}$$

The authentication overhead O is the extra bytes introduced for image authentication, for instance, it includes the hashes appended to the packets and the digital signature. So, the overhead $O(\pi)$ can be computed as in (5), where SIZ_{sig} and SIZ_{Hash} are the sizes of the signature and hash, respectively

$$O(\pi) = SIZ_{sig} + \sum_{P_m} |\pi_m| SIZ_{Hash}. \tag{5}$$

Before we compute the overall expected distortion D, we need to give a definition of authenticated image. A more restrictive definition is that the authenticated media must have exactly the same content and same quality as the original one. This is not realistic, because the received media will usually have degraded quality caused by network loss, even if no authentication is applied. A more realistic definition is that the authenticated media corresponds to the media decoded exclusively from the authenticated packets. This definition prevents packet alteration, but it assumes that network loss is not malicious, as loss is usually caused by network congestion. Under this definition, a packet is consumed only when it is received, decodable and authenticated. Throughout this paper, we use the latter definition based on the following considerations: obviously a received and decodable but unauthenticated packet should not be consumed because of security concern; however, an authenticated but undecodable packet is also meaningless for consumption (e.g., display). Using this definition, the expected distortion $D(\pi)$ can be calculated as in (6), assuming distortion is additive, where D_0 is the distortion when no packet is consumed, $\Delta(D_m$ is the amount by which the distortion will be reduced if the packet P_m is consumed, ρ_m denotes the probability that P_m is decodable, and $1-\varepsilon(\pi_m)$ denotes the probability that P_m is verifiable with π_m given that P_m is decodable

$$D(\pi) = D_0 - \sum_{P_m} \Delta D_m \rho_m [1 - \varepsilon(\pi_m)]. \tag{6}$$

IV. Optimized Content-Aware Authentication Scheme

The image authentication system for JPEG-2000 stream over a lossy channel is illustrated in Fig. 6. After encoding the original image, the sender signs the resulting JPEG-2000 codestream by constructing an authentication graph. Each JPEG-2000 packet has at least one path destined at the signature packet. This scheme is similar to the Gennaro and Rohatgi's scheme [13] except that each packet has a variable redundancy degree based on the distortion information. Once the authentication graph is built, the packets are transmitted over a lossy channel. The JPEG-2000 decoder accepts only those authenticated and decodable packets, and reconstructs the authenticated image.

In the image-authentication system, the most vital step is to sign the stream, i.e., to build the optimized authentication graph. In the rest of this section, we first introduce how to build an optimized authentication graph for JPEG-2000 streams, using the distortion-overhead optimization framework. This is followed by a simplified way of building the authentication graph with much lower complexity.

A. Distortion-Overhead Optimized Graph for JPEG-2000 Streams

Each JPEG-2000 packet is denoted by P_m^l, where the l is the layer number, and m is the index of the corresponding layer-0 packet, according to the progressive order of the JPEG-2000 codestream. The other quantities associated with P_m^l are also denoted in a similar way, like π_m^l, ΔD_m^l and ρ_m^l. Given a Lagrangian multiplier λ, we can solve the problem by finding the vector π that minimizes the expected Lagrangian in (7)

$$\begin{aligned} J(\pi) = D(\pi) + \lambda O(\pi) = D_0 + \lambda SIZ_{\text{sig}} \\ + \sum_{P_m^l} \left[\left(-\Delta D_m^l \rho_m^l \left(1 - \varepsilon(\pi_m^l) \right) \right) \right. \\ \left. + \lambda |\pi_m^l| SIZ_{\text{Hash}} \right]. \end{aligned} \tag{7}$$

Finding the optimized variable π is accomplished in two stages: the first stage is to determine π_m^l for high layer packets P_m^l, when l is greater than 0. The second stage is to determine π_m^0 for the packets P_m^0 in layer 0 (refer to Fig. 3).

1) Stage 1: Determine π_m^l when $l > 0$: In JPEG-2000, the high layer packet is not decodable unless all the corresponding lower layer packets are decodable and authenticated, i.e., the packet P_m^l depends on P_m^k for all k such that $0 \le k < l$, we say that P_m^l is a descendent of P_m^k and P_m^k is an ancestor of P_m^l. In this case, one hash link connecting P_m^l to one of its ancestors is sufficient, because we are interested in authenticating decodable packets only. In our scheme, the target node of the only hash

link from P_m^l is chosen to be its immediate ancestor P_m^{l-1}, i.e., $\pi_m^l = \{P_m^{l-1}\}$, because choosing other ancestors is not optimal in a rate-distortion sense. Given the fixed set of hash links from all packets other than P_m^l, $\pi_m^l = \{P_m^{l-1}\}$ will minimize the Lagrangian $J(\pi)$, as the resulting $\varepsilon(\pi_m^l)$ is equal to 0 and the redundancy degree $|\pi_m^l|$ takes the smallest value of 1. Therefore, when l is greater than 0, the set of outgoing hash links should be $\pi_m^l = \{P_m^{l-1}\}$ in order to obtain the optimized distortion-overhead performance. Note that an empty packet will not be involved in the graph construction, i.e., it does not contain any hash, and its own hash is not contained by any other packet.

2) Stage 2: Determine π_m^0 : After determining π_m^l for each high layer packet P_m^l (where $l \geq 1$), the probability ρ_m^l can be expressed as in (8), where ϕ_m^i denotes the probability that the packet P_m^i is received. In other words, the packet P_m^l is decodable if and only if all its ancestors (namely, $P_m^0, P_m^l, \ldots, P_m^{l-1}$) and P_m^l itself are received, and the corresponding layer-0 packet, P_m^0, is authenticated

$$\rho_m^l = \left(1 - \varepsilon\left(\pi_m^0\right)\right) \prod_{i=0}^{l} \phi_m^i. \tag{8}$$

Substituting (8) into (7), the Lagrangian $J(\pi)$ can be expressed as

$$\begin{aligned} J(\pi) = D_0 + \lambda SIZ_{sig} \\ + \sum_{P_m^l} \left[\left(-\Delta D_m^l \left(1 - \varepsilon\left(\pi_m^0\right)\right) \prod_{i=0}^{l} \phi_m^i \right) \right. \\ \left. + \lambda |\pi_m^l| SIZ_{Hash} \right]. \end{aligned} \tag{9}$$

To ensure the authentication graph is acyclic, we mandate that for hash links whose source packet is P_m^0, the target packet must be P_n^0 where $n < m$. At this stage, the goal is to find for each layer-0 packet the set of outgoing hash links that minimizes the Lagrangian $J(\pi)$. Note that if a packet in layer-0 is empty, the corresponding non-empty packet in higher layer is used in this stage. For instance, if both P_m^0 is empty and P_m^l are not empty, P_m^l will be used in the place of P_m^0. The straightforward method is exhaustive search, but its high computational complexity is not acceptable. A more practical approach is to use an iterative descent algorithm [21], where the objective function $J(\pi)$ is minimized one packet at a time, keeping the other packets unchanged, until convergence. For instance, let $\pi(0) = [\pi_0^0(0), \pi_1^0(0), \ldots]$ be the initial vector, and let $\pi(n) = [\pi_0^0(n), \pi_1^0(n), \ldots]$ be determined for $n = 1, 2, \ldots$, as follows. At iteration n, we select one packet, say, P_m^0, to find its π_m^0. For $k \neq m$, let $\pi_k^0(n) = \pi_k^0(n-1)$, while for packet P_m^0, let

$$\begin{aligned} \pi_m^0(n) &= \arg\min_{\pi'} J(\pi_0^0(n), \pi_1^0(n), \ldots, \pi', \ldots) \\ &= \arg\min_{\pi'} \mu_m^0 \varepsilon(\pi') + \lambda SIZ_{Hash} |\pi'| \end{aligned} \tag{10}$$

where (10) follows from (9) with (11), as follows:

$$\mu_m^0 = \sum_l \left(\Delta D_m^l \prod_{i \leq l} \phi_m^i \right). \tag{11}$$

TABLE I
PARAMETERS AND SEMANTICS OF THE PROPOSED AUTHENTICATION SCHEME

Parameters	Semantics
N	The number of segments. If N is 1, all lowest layer packets have the same redundancy degree.
γ_i	The redundancy degree of packets in Seg_i.
Z	The number of packets whose hashes are included in the signature packet.

At iteration n, we need to search for the set of outgoing hash links $\pi_m^0(n)$ that minimizes the Lagrangian. In subsequent iterations, the same process is repeated for different packets. The utility value μ_m^0 of the packet P_m^0, as expressed in (11), can be regarded as the amount by which the distortion will increase if P_m^0 is not verifiable given that it is decodable. Alternatively, we can interpret the utility value μ_m^0 as the partial derivative of (9) with respect to $\varepsilon(\pi_m^0)$. Therefore, the larger the utility value μ_m^0 is, the more attractive it is to decrease $\varepsilon(\pi_m^0)$.

During the optimization iterations, the Lagrangian $J(\pi)$ is non-increasing and has a lower bound of 0, so convergence is guaranteed. However, we cannot guarantee that it can reach a global minimal. To increase the chances of reaching the global minimal, one alternative solution is to invoke the optimization process with different initial vectors, and choose the resulting vector that incurs the smallest Lagrangian value.

B. Simplified Authentication Graph for JPEG-2000 Streams

Building the distortion-overhead optimized graph is computationally intensive because many iterations are required before convergence, and each iteration needs to search for the optimal set of hash links from the selected packet. In this section, we empirically build a simplified authentication graph which requires much lower computation complexity.

For the high-layer packets $P_m^l (l \geq 1)$, the set of outgoing hash links are exactly the same as the distortion-overhead optimized graph, i.e., P_m^l has only one outgoing hash link to P_m^{l-1}. For each packet P_m^0 in layer 0, we compute the utility value μ_m^0 using (11). After that, the packets are sorted into a list where the utility values are in descending order. The sorted list, denoted by *SL*, is then divided into N segments, namely, $Seg_0, Seg_{1...}, Seg_{N-1}$. Each packet in Seg_i has γ_i outgoing hash links whose target packets are randomly selected from the preceding packets in *SL*. The redundancy degree in consecutive segments is in decreasing order, i.e., $\gamma_0 > \gamma_1 > \cdots > \gamma_{N-1}$. There are a number of possible segmentation methods. One is based on equal segment size. Another method is based on utility value, e.g., Seg_i contains all packets with utility value falling in $[\mu_{\min} + i \times \eta, \mu_{\min} + (i+1) \times \eta)$, where $\mu_{\min}$ and μ_{max} are the lowest and highest utility value, respectively, and $\eta = (\mu_{max} - \mu_{min})/N$. The first method makes it easier to control the average redundancy degree, while the second method has slightly better performance, because its overhead allocation is more related to packets' utility value. The signature packet contains the hashes of the first Z packets in *SL*. The parameter Z is typically sufficient to be 3 and our experiment uses $Z = 3$.

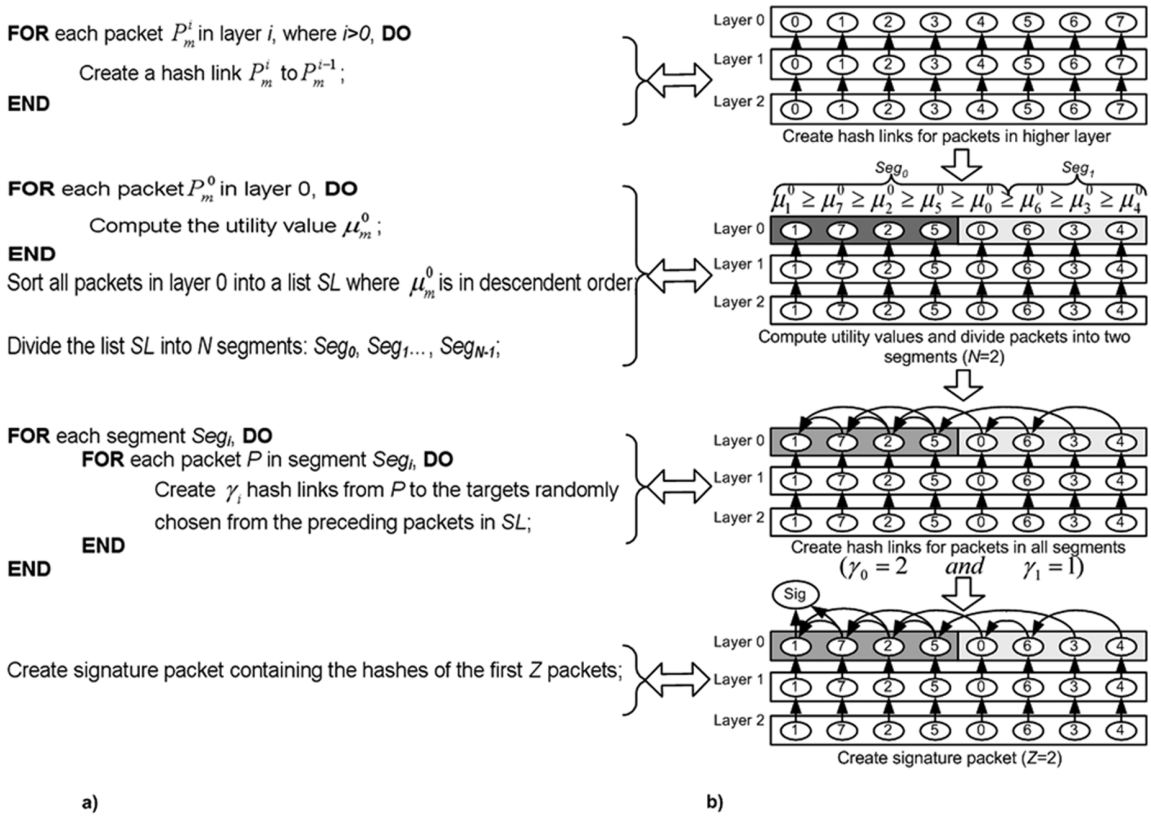

Fig. 7. Algorithm and example of constructing a simplified authentication graph. (a) Algorithm for constructing the simplified authentication graph. (b) Illustration of the steps constructing the simplified authentication graph

Table I summarizes the above parameters used for constructing the authentication graph. Through experiments, we found that it is typically sufficient to have equal-size segmentation, $N = 3$ and $\gamma_0 = \gamma_1 + 1 = \gamma_2 + 2$, where the redundancy degree is γ_1 on average.

The algorithm for constructing a simplified authentication graph is summarized in Fig. 7(a), which is illustrated in Fig. 7(b) using an example JPEG-2000 codestream with three layers and eight packets per layer, assuming that all packets are nonempty. This example uses the following parameters: $N = 2$, $\gamma_0 = 2$, $\gamma_1 = 1$, and $Z = 2$. First, for each high-layer packet $P_m^i (i > 0)$, a hash link is created from P_m^i to its immediate ancestor P_m^{i-1}. Second, for packets in layer 0, we compute their utility values, sort them and divide them into $N = 2$ segments with equal size. After that, for each packet in segment 0, $\gamma_0 = 2$ outgoing hash links are created with the target packet randomly chosen from the proceeding packets in the sorted list, and similarly for packets in segment 1. Finally, a signature packet is created containing the hash of the first two packets in the sorted list.

V. System Analysis

In this section, we analyze the content-aware stream authentication scheme and compare it with other existing schemes, in various aspects like computation overhead, communication overhead, verification probability, and the security.

A. Comparison With Existing Schemes

Since the proposed scheme is based on directed acyclic graph, we choose four existing graph-based schemes for comparison, including Simple Hash-chain [13], Authentication Tree [12], EMSS [14], Augmented Chain [15]. and Butterfly Authentication [16]. The performance criteria are summarized as follows.

1) Computation overhead: number of hash operations and signature operations required at the sender and receiver.
2) Communication overhead (bytes): average number of extra bytes carried by each packet for authentication purpose
3) Verification percentage: number of verified packets divided by the number of received packets.
4) Sender delay: delay at the sender (in number of packets) before the first packet can be transmitted.
5) Receiver delay: delay at the receiver (in number of packets) before the first packet can be verified and decoded.

Table II summarizes the performance of these six authentication schemes. The values are obtained based on the following assumptions.

1) A digital signature is amortized by a group of n packets.
2) h is the size of a hash and s is the size of a digital signature.
3) The authentication tree scheme uses a tree of degree two.
4) The augmented chain scheme is parameterized by variables a and p, which are named in [15] as the *chain length* and *packet buffer size* on the sender side, respectively.

In terms of computation overhead, the Authentication Tree scheme has to perform about n more hash operations than the other schemes. In terms of sender delay and receiver delay, the Augmented Chain scheme has the worst performance, while the other schemes are the same.

The Simple Hash-Chain has the smallest communication overhead (one hash per packet), but its verification probability is the lowest. On the other hand, Authentication Tree scheme

TABLE II
COMPARISON OF VARIOUS AUTHENTICATION SCHEMES

	Simple hash-chain	Authentication tree	EMSS	Augmented chain	Content-aware	Butterfly
Computation overhead	n,1	2n-1, 1	n+1, 1	n+1, 1	n+1, 1	n+1, 1
Communication overhead	h+s/n	s+$\log_2$n*h	Variable	2h+s/n	Variable	s/n+2h
Verification probability	Variable	1	Variable	Variable	Variable	Variable
Sender delay	n	n	1	p	n	n
Receiver delay	1	1	n	n	1	1

has the highest communication overhead but also the highest verification probability. These two schemes are the extreme cases (one favors communication overhead while the other favors verification probability), while all other schemes try to achieve a balance in-between. In particular, both EMSS and content-aware scheme can be configured with different overheads, resulting in different verification probabilities. The Augmented Chain and Butterfly Authentication scheme has fixed communication overhead. In this regard, EMSS and content-aware schemes are more flexible and generically applicable since their overhead levels are tunable.

The above comparisons are for streaming general data packets. However, for media streams, we should use different benchmark criteria. The most important performance measure should be the PSNR of the authenticated image rather than the verification probability of the delivered packets. In this regard, our content-aware scheme is more efficient than existing schemes due to two reasons.:

1) It eliminates all the unnecessary hash links that can only help to increase the verification probability, but do not help the PSNR of the authenticated image. For example, if packet P_i depends on P_j, it is sufficient to have a hash link from P_i to P_j, and any hash link from P_i to other packet does not help to improve the PSNR of the authenticated image.
2) The hash links are used in a more efficient manner. The more important packets have more outgoing hash links, which help to increase the PSNR, while the less important packets (which account for a large proportion of the total packets) have less outgoing hash links, resulting in smaller overhead.

B. Security Analysis

Similar to the existing graph-based authentication scheme, the content-aware scheme relies on the hash chain and digital signature. Therefore, the security strength of this scheme is the same as the underlying cryptographic algorithms. For example, SHA-1 can be used for one-way hashing and RSA can be used for signature generation and verification. For more details on security strength, refer to Merkle's tree authentication [18].

C. Utility Values

As every network has a MTU size, a packet has to be segmented into smaller datagrams for transmission. Therefore, the probability of receiving the packet P_m^l, ϕ_m^l, can be expressed in (12), where p_{lost} is the loss probability of the network datagram (here we assume i.i.d random loss) and R_m^l is the packet size in bytes

$$\phi_m^l = (1 - p_{\text{lost}})^{\lceil R_m^l / MTU \rceil}. \tag{12}$$

By substituting (12) into (11), we can see that the utility value, μ_m^0, is determined by the associated distortion ΔD_m^l, packet size R_m^l of its descendent packets, the loss probability p_{lost}, and MTU. If the packet size R_m^l is big, it needs more datagrams for transmission, thereby decreasing its probability of being received. So, given a fixed value for p_{lost} and MTU, the packet P_m^0 will have a greater utility value when its descendent packets have larger ΔD_m^l and smaller R_m^l.

The MTU value depends on the physical network links, e.g., Ethernet has a MTU of about 1500 bytes and the ATM network has a MTU of 53 bytes. When a communication path between two end hosts consists of different physical links, the smallest MTU can be discovered by the end host using the path MTU discovery protocol [22].

To derive the utility values, the sender also needs to know the network loss probability p_{lost}. The sender could presume a reasonable value for it, or could estimate it based on past communications. For instance, the real-time transport protocol (RTP) [23] specified the window-based measurement techniques for estimating the loss probability. However, for the simplified authentication graph, it is not important to have an accurate value for p_{lost}, because it does not change the relative order of the utility values in the sorted list *SL*.

VI. EXPERIMENTAL RESULTS

This section experimentally compares our content-aware scheme against EMSS, Augmented Chain, and Butterfly authentication schemes using JPEG-2000 images to further demonstrate the validity of our proposed scheme.

We implemented five schemes, namely, *WITHOUT_AUTH*, *EMSS_AUTH, C_A_AUTH, AC_AUTH*, and *BUTTERFLY_AUTH*. The first scheme, *WITHOUT_AUTH*, is

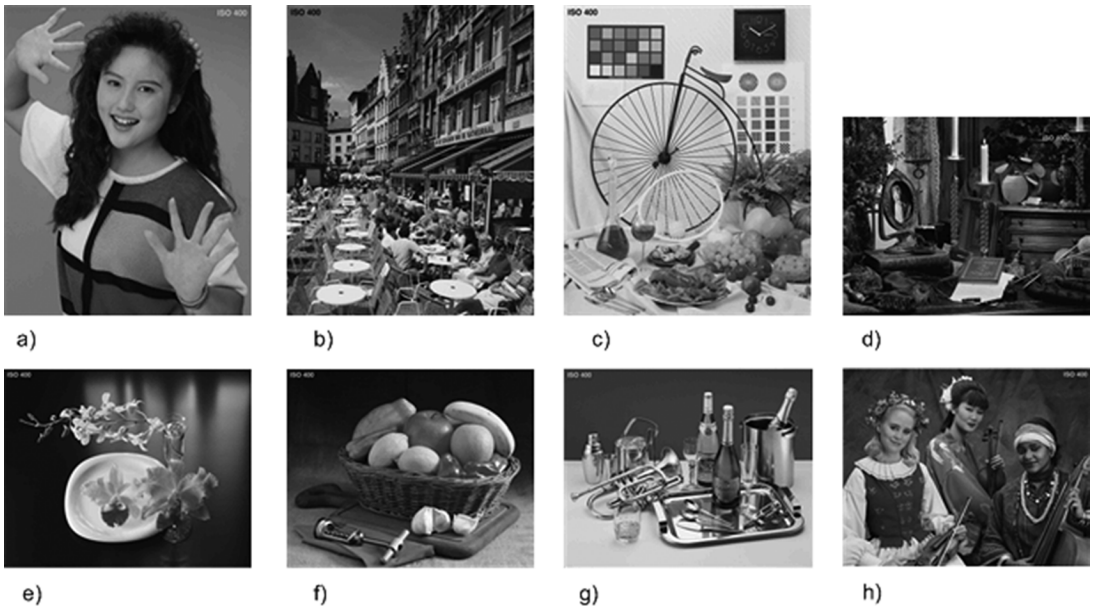

Fig. 8. Testing images used in our experiments. (a) Woman 2048 × 2560. (b) Cafe 2048 × 2560. (c) Bike 2048 × 2560. (d) Bride 2560 × 2048. (e) Flower 2560 × 2048. (f) Fruits 2560 × 2048. (g) Bottles 2560 × 2048. (h) Actors 2560 × 2048.

to simply send the packets in the order they appear in the JPEG-2000 codestream, and no authentication is applied. This scheme provides a reference for the achievable distortion performance if verification is not required. Note that this scheme provides an upper bound on the performance of all authentication schemes. The second scheme, *EMSS_AUTH*, implements the EMSS authentication [14], where every packet has the same redundancy degree. The third scheme, *C_A_AUTH*, implements the proposed content-aware authentication using the simplified authentication graph as proposed in Section III. Through simulation, we found that the content-aware scheme yields good performance when the parameter N is 3. Further increasing N does not produce substantial performance improvement, because its performance is already quite close to the upper bound when N is set to 3. The fourth scheme, *AC_AUTH*, implements the Augmented Chain, and the fifth scheme, *BUTTERFLY_AUTH*, implements the butterfly authentication. For all schemes, the packets are sent in the order they appear in JPEG-2000 codestreams, while the signature packet is sent multiple times to minimize its loss probability.

The network is modeled by an i.i.d distribution, where the average loss probability ranges from 0 to 0.15. In addition, MTU is set to 1500 bytes, as used by Ethernet. Our experiment uses the eight JPEG-2000 testing images (each 2560 × 2048 pixels). Each image has four resolution levels and 260 packets per layer, and we vary the number of layers in the experiments. The testing images used in our experiments are shown in Fig. 8.

The first experiment is to demonstrate the effectiveness of the authentication redundancy adapted to the distortion. The JPEG-2000 images are encoded with only one layer, so *C_A_AUTH* can take advantage of the distortion information but not the layer structure. For *C_A_AUTH*, the parameters are set as follows: $N = 3$, $\gamma_0 = 3$, $\gamma_1 = 2$, $\gamma = 1$, and $Z = 6$, so the redundancy degree is 2 on average. The other schemes use

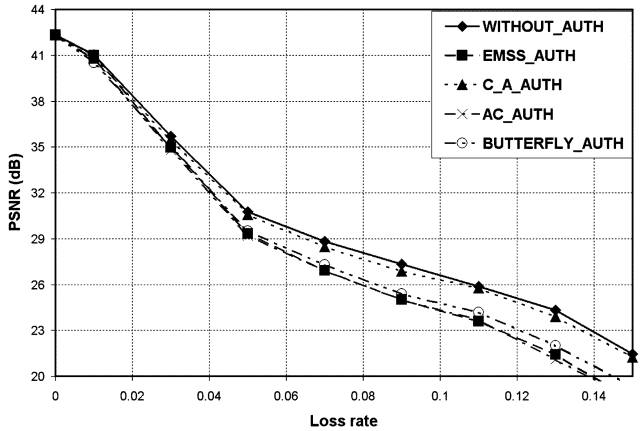

Fig. 9. PSNR at various loss rates (2 hashes/packet on average, with one layer).

a similar level of redundancy. Fig. 9 gives the PSNR of the five schemes. *C_A_AUTH* consistently outperforms the other schemes at all network loss rates. In fact, the PSNR curve of *C_A_AUTH* is very close to that of *WITHOUT_AUTH*, which achieves our original design goal, because the authentication overhead is added in an optimized manner.

Fig. 10 shows the verification probabilities of the four authentication schemes. When the loss rate is less than 0.1, *C_A_AUTH* has a slightly lower verification probability, because one third of the packets have redundancy degree of 1. When the loss rate is larger than 0.1, a flat redundancy degree of 2 for all packets is not enough, which causes a dramatic decrease for *EMSS_AUTH, AC_AUTH* and *BUTTERFLY_AUTH*. For *C_A_AUTH*, such a decrease is relatively small because one third of the packets still have redundancy degree of 3.

From Figs. 9 and 10, we can see that although *C_A_AUTH* sometimes has lower verification probability than the other authentication schemes, it produces higher PSNR. The

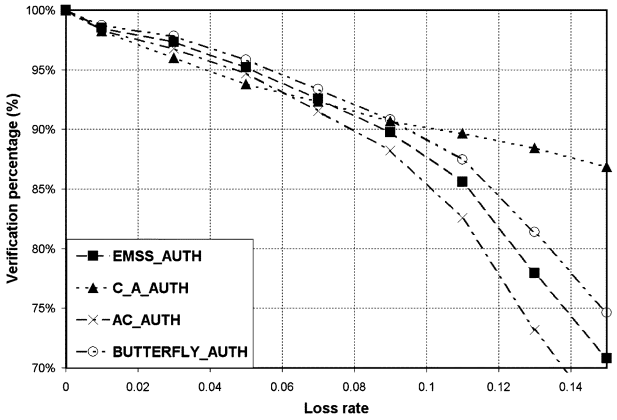

Fig. 10. Verification probabilities at various loss rates (2 hashes/packet on average, with one layer).

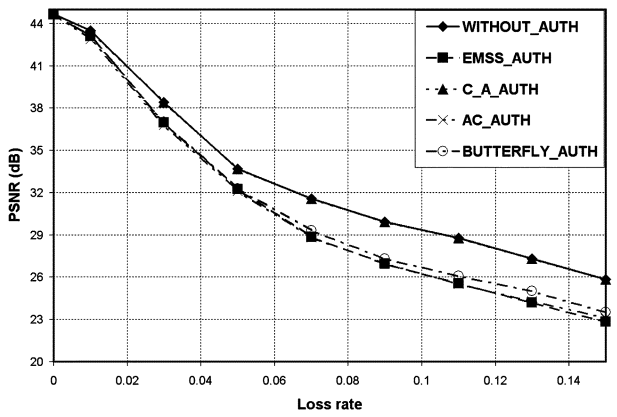

Fig. 11. PSNR at various loss rates (2 hashes/packet on average, with six layers).

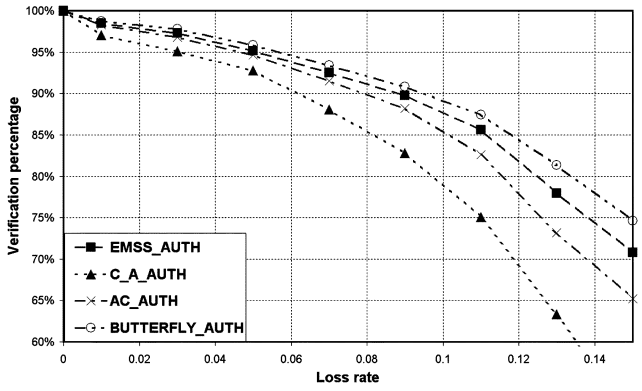

Fig. 12. Verification probabilities at various loss rate (2 hashes/packet on average, with six layers).

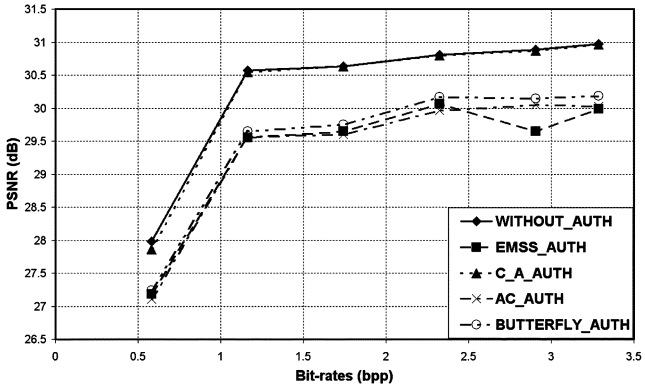

Fig. 13. PSNR at various bit-rates (loss $\mathrm{rate} = 5\%$, 2 hashes/packet on average, with six layers).

C_A_AUTH is able to achieve near distortion-overhead optimized performance, as the authentication overhead is added in a more cost-effective manner. The packets are differentiated according to their importance, more important packets have higher verification probability and less important packets have lower authentication overhead.

The second experiment is to evaluate the proposed system when both distortion and layer structure are utilized. Accordingly, the JPEG-2000 codestreams are encoded with six layers. Thus, *C_A_AUTH* is able to take advantage of both the layer structure and the distortion information, but the other schemes are agnostic to both. The parameters for this experiment are the same as that for the previous experiment. Fig. 11 shows the PSNR curves of the three systems, which is similar to those in Fig. 9.

Fig. 12 compares the verification probabilities of the four authentication schemes. The *C_A_AUTH* has significantly lower verification probability than the other schemes. This is because higher layer packets have redundancy degree of only one in *C_A_AUTH*, resulting in lower verification probability.

From the results of the previous two experiments (Figs. 9,10, 11, and 12), we can conclude that *C_A_AUTH* has PSNR very close to *WITHOUT_AUTH*. In addition, it consistently outperforms the other scheme in terms of PSNR, even though it may have lower verification probability.

The third experiment evaluates the PSNR versus bit-rate curve for transmitting the authenticated image over a lossy network. The JPEG-2000 codestreams are also encoded with six layers. All authentication schemes have the same average redundancy degree of 2. The network loss probability is set to 0.05, because higher loss probability will flatten the rate-PSNR curve. All other parameters are the same as in the second experiment. Fig. 13 shows the PSNR curves. Again, at all image bit-rates, *C_A_AUTH* achieves a PSNR close to *WITHOUT_AUTH*. It consistently outperforms the other schemes.

The fourth experiment is to compare the performance of the four authentication schemes at various overhead levels. Again, we set the loss probability to 0.05. The JPEG-2000 images are encoded with one layer, because we want *C_A_AUTH* to utilize the distortion information but not the layer structure. We measure the PSNR at various overhead levels, ranging from one to six hashes per packet. Fig. 14 shows that at loss rate 0.05, the proposed scheme outperforms the other schemes when the redundancy degree is less than 3. When the loss rate is higher, the improvement of the proposed scheme over the other schemes will be further increased.

The fifth experiment is to measure the minimum overhead required to achieve a PSNR that is 99% of *WITHOUT_AUTH*. The JPEG-2000 codestreams have one layer, for the same reason as the previous experiment. As shown in Fig. 15, *C_A_AUTH*

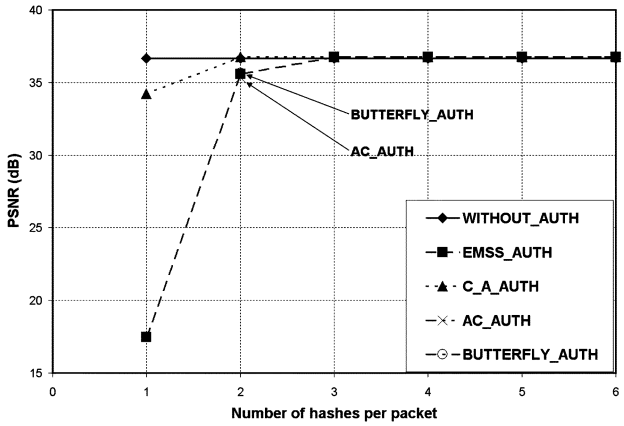

Fig. 14. PSNR at various redundancy degrees (loss rate $= 0.05$, with one layer).

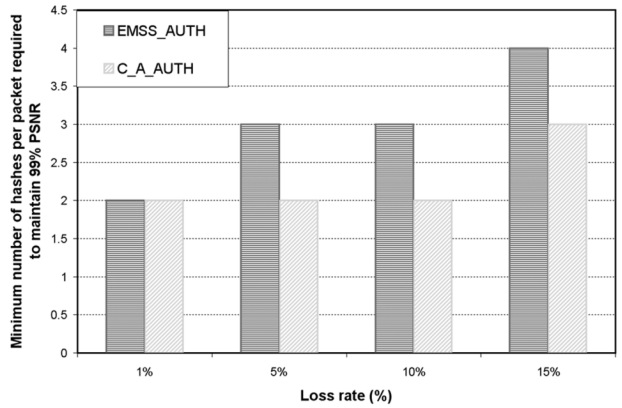

Fig. 15. Minimum overhead required to achieve 99% PSNR at various loss rates (with one layer).

requires the overhead to be two hashes per packet when the loss rate is not greater than 0.1, and requires the overhead to be three hashes per packet otherwise. However, *EMSS_AUTH* requires much more overhead in order to maintain the same PSNR level.

VII. Conclusions

In this paper, we have proposed an optimized content-aware authentication scheme, which is able to achieve distortion-overhead optimization by utilizing information about the coding structure and media content collected from the JPEG-2000 encoding process. The main contributions of this paper are summarized as follows.

1) For the authenticating media stream delivered over a lossy network, instead of optimizing the verification probability, we focus on optimizing authenticated media quality.
2) We proposed a distortion-overhead optimization framework for media authentication. Given a specific authentication overhead level, the proposed scheme computes an authentication graph that minimizes the distortion of the authenticated image at the receiver. Alternatively, given desired authenticated image quality, the proposed scheme computes the authentication graph that minimizes the authentication overhead.
3) In view that the optimization process has high computational complexity, we also proposed a simplified authentication graph construction that requires much lower complexity to compute. Through system analysis and simulation, we demonstrated that the proposed scheme achieves a rate-distortion (R-D) curve of the authenticated image, which is very close to the R-D curve when no authentication is required, and it substantially outperforms existing schemes at all bit rates and loss probabilities.

Our future work will extend the current scheme to other media streaming applications such as audio and video, and take more sophisticated network conditions into consideration.

References

[1] Information Technology—JPEG2000 Image Coding System, ISO/IEC International Standard 15444-1 2000, ITU Rec. T.800.
[2] D. Taubman, "Remote browsing of JPEG-2000 images," in *Proc. IEEE Int. Conf. Image Processing*, Rochester, NY, 2002.
[3] S. Deshpande and W. Zeng, "Scalable streaming of JPEG-2000 images using hypertext transfer protocol," in *ACM Multimedia*, Oct. 2001.
[4] R. Qiu and W. Yu, An Efficient Quality Scalable Motion-JPEG2000 Transmission Scheme Dept. Comput. Sci., Washington Univ., St. Louis, MO, 2001, Tech. Rep. WUCS-01–37.
[5] Information Technology—JPEG2000 Image Coding System—Part 9: Interactivity Tools, APIs and Protocols, ISO/IEC International Standard 15444-9 2004, ITU Recommendation T.800.
[6] JPEG 2000 Image Coding System—Part 8: JPEG 2000 Security—Final Committee Draft 2004, ISO/IEC JTC1/SC29/WG1 N3480.
[7] JPEG 2000 Image Coding System—Part 11: Wireless JPEG 2000—Final Commission Draft 2005, ISO/IEC JTC1/SC29/WG 1 N3573.
[8] S. Wee and J. Apostolopoulos, "Secure scalable streaming and secure transcoding with JPEG-2000," in *Proc. IEEE Int. Conf. Image Processing*, Barcelona, Spain, Sep. 2003.
[9] ——, "Secure transcoding with JPSEC confidentiality and authentication," in *Proc. IEEE Int. Conf. Image Processing*, Singapore, Oct. 2004.
[10] Z. Zhang, G. Qiu, Q. Sun, X. Lin, Z. Ni, and Y. Q. Shi, "A unified authentication framework for JPEG2000," in *Proc. IEEE Int. Conf. Multimedia & Expo*, Taipei, Taiwan, R.O.C., Jun. 2004.
[11] Q. Sun, S. Ye, C.-Y. Lin, and S.-F. Chang, "A crypto signature scheme for image authentication over wireless channel," *Int. J. Image and Graph.*, vol. 5, no. 1, pp. 1–14, 2005.
[12] C. K. Wong and S. Lam, Digital Signatures for Flows and Multicasts Univ. Texas at Austin, Dept. Comput. Sci., 1998, Tech. Rep. TR-98-15.
[13] R. Gennaro and P. Rohatgi, "How to sign digital streams," in *Advances in Cryptology—CRYPTO '97*, pp. 180–197.
[14] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proc. IEEE Symp. Security and Privacy*, 2000, pp. 56–73.
[15] P. Golle and N. Modadugu, "Authenticating streamed data in the presence of random packet loss," in *ISOC Network and Distributed System Security Symp.*, 2001, pp. 13–22.
[16] Z. Zhang, Q. Sun, and W.-C. Wong, "A proposal of butterfly-graph based stream authentication over lossy networks," in *Proc. IEEE Int. Conf. Multimedia & Expo*, The Netherlands, Jul. 2005.
[17] B. Schneier, *Appl. Cryptog.*. : Wiley, 1996, pp. 429–502.
[18] R. C. Merkle, "A certified digital signature," in *Advances in Cryptology—CRYPTO'89*, 1989, pp. 218–238.
[19] D. Taubman and M. W. Marcellin, *JPEG2000: Image Compression Fundamentals, Standards and Practice*. Dordrecht, The Netherlands: Kluwer, 2001, pp. 375–379.
[20] M. Rabbani and R. Joshi, "An overview of the JPEG2000 still image compression standard," *Signal Process.: Image Commun.*, vol. 17, pp. 3–48, Jan. 2002.
[21] R. Fletcher, *Practical Method of Optimization*, 2nd ed. New York: Wiley, 1987.
[22] J. Mogul and S. Deering, "Path MTU discovery," in *RFC 1191*, Nov. 1990.
[23] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: A transport protocol for real-time applications," in *RFC 3550*, Jul. 2003.

Zhishou Zhang (S'02) received the Bachelor's (Hons.) degree from the School of Computer Engineering, Nanyang Technological University, Singapore, in 1998, and the Master's degree in 2002 from the School of Computing, National University of Singapore, where he is currently pursuing the Ph.D. degree in the Department of Electronic and Computer Engineering.

Since 2000, he has been a Researcher with the Institute for Infocomm Research, Singapore, a national research institute under the Agency for Science, Technology and Research. He actively participates in standardization activities for JPEG committee and serves as a co-editor for JPEG-2000 File Format Security (FFSEC). His research interests are in media security and media communication systems.

Qibin Sun (M'97) received the Ph.D. degree in electrical engineering from the University of Science and Technology of China (USTC) in 1997.

Since 1996, he has been with the Institute for Infocomm Research, Singapore, where he is responsible for industrial, as well as academic, research projects in the areas of media security, image, and video analysis. He is currently leading the Media Understanding Department, conducting research and development in media (text, audio, image, video) analysis, retrieval, and security. He is also the Head of Delegates of Singapore for ISO/IEC SC29 WG1(JPEG). He was a Research Scientist with Columbia University, New York, during 2000-2001.

Dr. Sun actively participates in professional activities such IEEE ICME, IEEE ISCAS, IEEE ICASSP and ACM MM, etc. He serves as a member of the Editorial Board for *IEEE Multimedia Magazine* and for *LNCS Transactions on Data Hiding and Multimedia Security*, and as an Associate Editor of IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY.

Wai-Choong (Lawrence) Wong (SM'93) received the B.Sc. (Hons.) and Ph.D. degrees in electronic and electrical engineering from Loughborough University, Leicestershire, U.K.

Since November 2002, he has been the Executive Director of the Institute for Infocomm Research, Singapore, a national research institute under the Agency for Science, Technology and Research. He is also a Professor with the Department of Electrical and Computer Engineering, National University of Singapore (NUS). Before joining NUS in 1983, he was a Member of Technical Staff at the Crawford Hill Laboratory, AT&T Bell Laboratories, Holmdel, NJ, from 1980 to 1983. He has published over 170 papers in international journals and conferences. He also co-authored the book *Source-Matched Mobile Communications* (London, U.K.: Pentech Press, 1995). His research interests are in wireless communication systems, including *ad hoc* and sensor networks, and multimedia signal processing and compression.

Dr. Wong was a recipient of the IEE Marconi Premium Award in 1989, the IEEE Millenium Award in 2000, and the e-innovator Award in 2000.

John Apostolopoulos (M'91–SM'97) received the B.S., M.S., and Ph.D. degrees from Massachusetts Institute of Technology, Cambridge.

He joined Hewlett-Packard Laboratories, Palo Alto, CA, in 1997, where he is currently a Principal Research Scientist and Project Manager for the Streaming Media Systems Group. He also teaches at Stanford University, Stanford, CA, where he is a Consulting Assistant Professor of Electrical Engineering. He contributed to the U.S. Digital Television and JPEG-2000 Security (JPSEC) standards. His research interests include improving the reliability, fidelity, scalability, and security of media communication over wired and wireless packet networks.

Dr. Apostolopoulos served as an Associate Editor of the IEEE TRANSACTIONS ON IMAGE PROCESSING and the IEEE SIGNAL PROCESSING LETTERS, and currently serves as Vice-Chair of the IEEE Image and Multidimensional Digital Signal Processing (IMDSP) Technical Committee. Recently, he was also co-guest editor of the Special Issue on Multimedia over Broadband Wireless Networks of *IEEE Network* and a General Co-Chair of VCIP'06. He received a Best Student Paper award for part of his Ph.D. dissertation, the Young Investigator Award at VCIP 2001 for his paper on multiple description video coding and path diversity for reliable video communication over lossy packet networks, and in 2003 was named "one of the world's top 100 young (under 35) innovators in science and technology" (TR100) by *Technology Review*.

Susie Wee (M'96–SM'05) received the B.S., M.S., and Ph.D. degrees in electrical engineering from the Massachusetts Institute of Technology (MIT), Cambridge.

She is the Director of the Mobile and Media Systems Lab, Hewlett-Packard (HP) Laboratories, Palo Alto, CA, where she is responsible for research programs in multimedia, networked sensing, next-generation mobile multimedia systems, and experience design. Her laboratory conducts activities in the U.S., Japan, and England, and includes collaborations with partners around the world. Her research interests broadly embrace the design of mobile streaming media systems, secure scalable streaming methods, and efficient video-delivery algorithms. In addition to her work at HP Labs, she is a Consulting Assistant Professor at Stanford University, Stanford, CA and is currently a co-editor of the JPEG-2000 security standard (JPSEC).

Dr. Wee served as an Associate Aditor for the IEEE TRANSACTIONS ON IMAGE PROCESSING and IEEE TRANSACTIONS ON CIRCUITS, SYSTEMS, AND VIDEO TECHNOLOGY. She received *Technology Review's* Top 100 Young Investigators award in 2002.