A Practical Progressive Authentication Scheme for JPEG 2000 Codestreams

Marielena PALACIOS PEREZ, Masaaki FUJIYOSHI, and Hitoshi KIYA
Tokyo Metropolitan University, Hino-shi, Tokyo 191–0065, Japan
E-mail: palaciosperez-marielena@sd.tmu.ac.jp, mfujiyoshi@m.ieice.org, kiya@sd.tmu.ac.jp

***Abstract*—This paper proposes an authentication scheme for JPEG 2000 (JP2) codestreams with multiple dimensions of hierarchical scalability. The proposed scheme progressively authenticates received JP2 packets in groups of packets (GoP) to serve hierarchical scalability in practice. This scheme compares original and reference signatures to detect tampering of a codestream in which a reference signature is regenerated from the received GoP. Original signatures are generated before sending the codestream and are stored throughout codestreams so that the scheme fits the progressive decoding of JP2 images. The proposed scheme remains JP2 codestream compliance and does not add distortion to signed codestreams. It also takes account into multiple dimensions of hierarchical scalability, whereas the conventional scheme allows one scalability. Experimental results show the effectiveness of the proposed scheme.**

I. Introduction

Digital contents are not as secure as they should be. Images, for example, are vulnerable to tampering. Sometimes, it is difficult for humans to detect tampering when an original and tampered images are compared. Therefore, image authentication schemes are required to ensure image integrity [1]. An image authentication scheme detects intentional modifications using digital signature [2], robust hash [3] or non-intrusive schemes that do not process images when they are created [1].

Digital signatures can be hidden in the image itself using fragile watermarking [4], or they can be transmitted along with the image [4]. This paper focuses on the latter. In digital signature-based image authentication schemes, a digital signature is generated from an image. Afterwards, the signature is compared with a reference signature, which is computed from the image that is being authenticated. If the image has been tampered, the reference signature will differ from the original; otherwise, the image is correctly authenticated (genuine).

Meanwhile, digital images are often compressed for efficient transmission and/or storing. JPEG 2000 (JP2) [5]–[7] is an international standard for multimedia compression, and it is known for its set of useful features like hierarchical scalability as well as its superior compression performance. For such progressive compressed images, progressive authentication schemes have been proposed [8]–[13], but they only take account into one dimension of hierarchical scalability or require a processing each JP2 packets.

In this paper, a new image authentication scheme taking accounts into multiple dimensions of hierarchical scalability for JP2 codestreams. Though JP2 allows us to compress an image with multiple dimensions of hierarchical scalability (until four dimensions of progressivity) scalable decoding patterns fewer than the possible patterns are executed in practice. This paper introduces *groups of JP2 packets* (GoPs) to fill in the gaps between the theoretically possible and actual decoding patterns. The proposed scheme authenticates a codestream in GoPs.

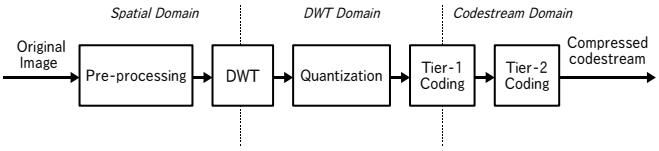


Fig. 1. JPEG 2000 encoder.

This paper is organized as follows. Section II overviews the JP2 standard. Section III presents the proposed authentication scheme, and the experimental results are shown in Section IV. Finally, conclusions are drawn in Section V.

II. JPEG 2000 Overview

This section outlines the JP2 standard [5]–[7]. Its encoding process, codestream structure, and progressive decoding are further mentioned.

A. Encoding Process

A JP2 encoder is illustrated in Fig. 1. An original image, first, may be spatially divided into blocks referred to as tiles which will be independently encoded. Furthermore, a level shifting of pixel values and a color transformation are applied to one or more tile(s) before applying discrete wavelet transformation (DWT). In case of lossy compression, quantization is applied to DWT coefficients. DWT coefficients are further divided into blocks referred to as codeblocks. Here, a codeblocks is a unit for encoding. Finally, the adaptive binary arithmetic encoding known as Tier-1 encoding and the codestream organizing (Tier-2 coding) are adopted. Subsequent sections further mention the codestream structure and the progressive decoding.

B. Codestream Organization

Figure 2 shows the JP2 codestream structure. A JP2 codestream begins with a main header followed by a sequence of tile streams and a marker segment called EOC (end of codestream) at the end. Each tile stream is composed of a tile header and a set of part streams which consist of JP2 packets

ISBN: 978-602-8944-11-3

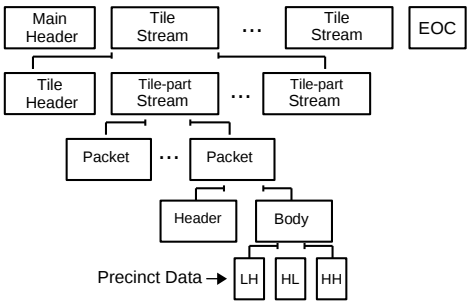


Fig. 2. JPEG 2000 codestream structure.

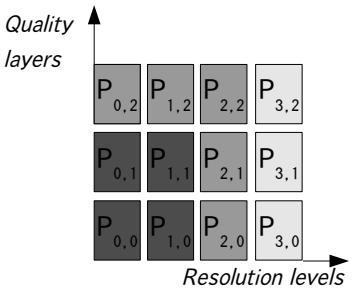


Fig. 4. Groups of JPEG 2000 packets. Different colors for different groups.

of coded data. Header and body data are included in each JP2 packet. JP2 packets are compound of data belonging to a specific color component, resolution level, quality layer, and precinct. Precincts are composed of set of arithmetic encoded codeblock from a resolution, which belongs to the same spatial region.

C. Progressive Decoding

In progressive systems, data are transmitted, stored, and/ or displayed according to a previously defined sequence. As more data arrived, the better the image is visible in a progressive decoding. This scalable characteristic is useful for receiving data over slow transmission links, in access control applications, in device-based contents adaptations, and so on [6], [7]. The JP2 standard allows images to be compressed using four dimensions of progressive scalability: quality layers (L), resolution levels (R), precincts (P), and color components (C) [5]–[7].

In JP2, progressions are performed by ordering packets using a collection of nested loops. Five progression orders are supported in JP2: LRCP, RLCP, RPCL, PCRL, and CPRL, where the order of the initials of the four dimensions L-R-C-P indicate the hierarchy of nesting governing the progression. For example, in LRCP progression (Fig. 3 (a)), JP2 packets from quality layer zero appear first in the codestream for every resolution levels, color components, and precincts. Then, JP2 packets from quality layer one and so on will appear throughout the codestream.

In Digital Cinema [14], however, only two types of JP2 distributions are used : namely, 2k (2048×1080 pixels per frame) and 4k (4096×2160 pixels per frame) formats. Decoder shall be able to firstly decode packets for the 2k size, and then decode packets for the 4k size in case of existing to improve the final visual quality of frames.

That is, in practical applications, a JP2 coded image is decoded in a fewer progression levels than the possible progression levels achieved by JP2 packet combinations in a decoding process. This paper focuses this gap and introduces the groups of JP2 packets (GoPs) to describe this fact; a GoP consists of JP2 packets simultaneously decoded. An example of the concept is shown in Fig. 4 where 12 of JP2 packets form three different GoPs.

The next section proposes a progressive authentication scheme for JP2 encoded images. The proposed scheme signs codestreams and detects tampering in GoPs.

III. Proposed Scheme

This section proposes a progressive codestream domain authentication scheme for JP2 coded images. The proposed system is shown in Fig. 5. An original image is compressed by a standard JP2 encoder, and the compressed codestream is signed without being decompressed. Therefore, a suspected codestream is examined in the codestream domain.

Hereafter, the GoP setting shown in Fig. 4 is considered as the reference; three different shadow colors indicate three different GoPs which correspond to a bi-dimensional progression of four resolution levels and three quality layers. Subsequently

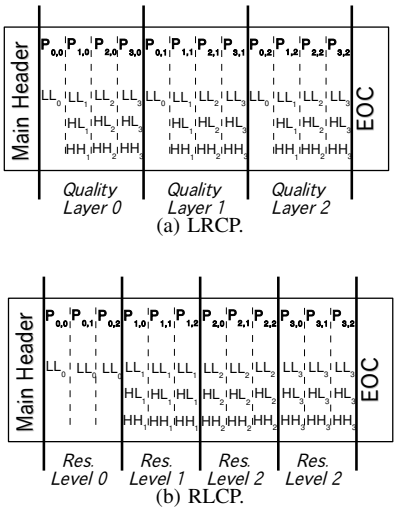


Fig. 3. JP2 packets form a codestream according to the progression order.

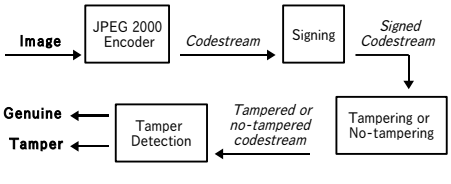


Fig. 5. The proposed system.

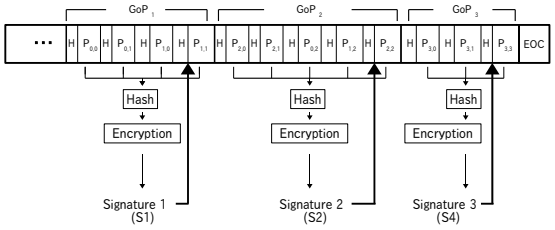


Fig. 6. Signing of a JP2 codestream (H indicates a JP2 packet header).

three sections describe signing, authentication and the features f the proposed scheme, respectively.

A. Signing

Figure 6 illustrates the concept of the signing in the proposed scheme. The proposed scheme applies a hash function to each GoP throughout a codestream, and it encrypts the obtained hash values with a key. In the reference GoP setting shown in Fig. 4, the first GoP is compound of four JP2 packets, the second has five, and the last one consists of three, so the proposed scheme applies a hash function to first four JP2 packets, middle five JP2 packets, and last three JP2 packets in Fig. 6.

The encrypted hash values are gathered to form a signature, which is inserted into the codestream. The proposed scheme inserts termination marker, that are two bytes value greater than 0xFF8F, and the encrypted signature after the last packet header of each GoP. Therefore, each GoP can be independently verified later.

B. Authentication

The proposed scheme firstly search an inserted signature with a termination marker. When no signature is found, the proposed scheme immediately determines that the codestream is inauthentic.

The codestream with the signature, then, is further examined as shown in Fig. 7. The proposed scheme extracts the inserted original signature and decrypts it with the same key used in the signing process so that the original signature can be compared with a reference signature. The reference signature is obtained by applying the same hash function used in the signing process to the corresponding GoP. When the original and reference signatures are the same in a GoP, the proposed scheme determines that the GoP of the codestream is genuine. Otherwise, the GoP is tampered.

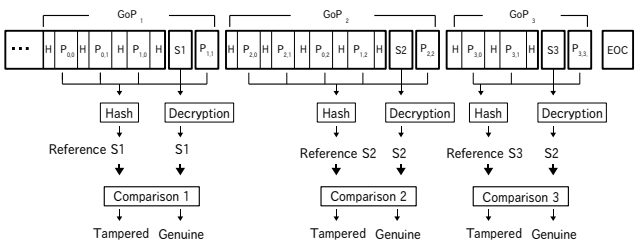


Fig. 7. Verification of a JP2 codestream (H indicates a JP2 packet header).

C. Features

This section describes the three principal features of the proposed scheme: progressive authentication for multiple dimensions of hierarchical scalability, codestream domain processing, and codestream structure compliant.

1) Progressive authentication for Multiple Dimensions of Hierarchical Scalability: Since the JP2 standard serves several progression throughout a codestream, an authentication taking account into multidimensional scalability is needed. The proposed scheme authenticates GoPs which are compound of two or more dimensions of scalability (quality layer, resolution, color component, precinct); in other words, it progressively authenticates JP2 packets with multiple dimensions of scalability.

2) Codestream Domain Processing: As mentioned above, the proposed scheme signs codestreams in the codestream domain. A merit of codestream domain processing is that there is no need of decompressing a codestream to authenticate it: the original signatures of a GoP and JP2 packets for computing the reference signature are both accessible in the codestream domain.

Moreover, codestreams are compound of binary data delimited by marker segments. In other words, codestream processing imply binary operations which are faster and less complex (low computational cost) than other numerical operations.

It is concluded that the proposed scheme works without decoding codestreams to the DWT or spatial domain for processing.

3) Codestream Structure Compliant: The proposed scheme takes account into the codestream structure for compliance with JP2 standard. The proposed scheme applies a hash function to a codestream segment corresponding to a GoP, and it does not change the segment itself. A signature composed of hash values is inserted after the last packet header of each GoP. In the signature insertion, termination marker is also inserted just before the signature so that a standard JP2 decoder skips the signature rather than decoding it. That is, decoding a signed codestream with a standard decoder restores the original decoded image without any distortion.

Consequently, the proposed scheme is compliant with JP2 codestream structure.

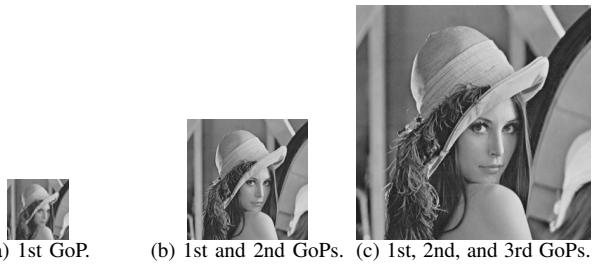
IV. Experimental Results

The effectiveness of the proposed scheme is verified in this section from the perspective of tamper detection ability and signature overhead. One of 256 levels of grayscale image with 512×512 pixels "Lena" shown in Fig. 8 is used for evaluation. A standard JP2 encoder implemented by Kakadu v6.0 compresses original Lena with four levels of decomposition and three quality layers. Lossy compression is performed. The codestream is signed using SHA-1 hash function [15], [16] and AES encryption [16], [17] in cipher feedback block cipher mode.

Fig. 8. Original Lena.

Here the reference GoP setting shown in Fig. 4 is assumed as the GoP setting. For Lena compressed with the reference GoP setting, signature lengths are summarized in Table I. The signature size depends on the number of GoPs, in other words, it not depends on either the image size or the number of packets throughout the codestream.

Figure 9 shows the results of a progressive authentication of the previously signed codestream. Figure 9 (a) is decoded after the 1st GoP is authenticated, Fig. 9 (b) is decoded with the authenticated 1st and 2nd GoPs, and Fig. 9 (c) is obtained from all authenticated GoPs.



(a) 1st GoP. (b) 1st and 2nd GoPs. (c) 1st, 2nd, and 3rd GoPs.

Fig. 9. Progressive authentication.

All genuine codestreams should have an appended signature in the proposed system, so the proposed scheme determines any unsigned codestreams inauthentic. Moreover, the proposed scheme also detects tampers for codestreams with a preserved signature and an imitation signature. Since the encryption key is securely stored, tampering in transformed or spatial domain after decoding a codestream will be detected though preserved signatures or imitation signatures are inserted to the regenerated codestream.

V. Conclusions

This paper has presented a progressive authentication scheme for JP2 coded images. In the scheme, signing and tamper detection are performed in the codestream domain. JP2 compliance is remained while a standard decoder is able to decompress the signed codestream without introducing any distortion to the decoded image. The scheme takes account into multidimensionally hierarchical scalability of JP2. Experimental results showed the effectiveness of the proposed scheme.

TABLE I
Signature size for Lena.

GoP	Packet ($p_{l,r}$)	Signature size (KiB)
1	$p_{0,0}$, $p_{0,1}$, $p_{1,0}$, and $p_{1,1}$	0.0195
2	$p_{0,2}$, $p_{1,2}$, $p_{2,0}$, $p_{2,1}$, and $p_{2,2}$	0.0195
3	$p_{3,0}$, $p_{3,1}$, and $p_{3,3}$	0.0195
Total size of signatures (KiB)		0.0583

References

[1] S. Lion, D. Kanellopus, and G. Ruffo, "Recent advances in multimedia information system security," *Informatica (Ljubljana)*, vol.33, pp.3–24, Mar. 2009.

[2] A. Haouzia and R. Noumeir, "Methods for image authentication: a survey," *Multimedia Tools and Applications*, vol.39, no.1, pp.1–46, Aug. 2008.

[3] C. Rey and J.L. Dugelay, "A survey of watermarking algorithms for image authentication," *EURASIP J. Applied Signal Process.*, vol.2002, pp.613–621, Jun. 2002.

[4] I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, and T. Kalker, "Digital watermarking and steganography," 2nd ed., Morgan Kufmann, 2008.

[5] ISO/IEC IS 15444-1: "Information technology — JPEG 2000 image coding system — Part 1: core coding system," 2004.

[6] D.S. Taubman and M.W. Marcellin, "JPEG 2000: image compression fundamentals, standards and practice," Kluver Academic Publishers, 2002.

[7] P. Schelkens, A. Skodras, and T. Ebrahimi, "The JPEG 2000 suite," Wiley, 2009.

[8] R. Grosbois, P. Gerbelot, and T. Ebrahimi, "Authentication and access control in the JPEG 2000 compressed domain," in *Proc. SPIE*, vol.4472, 2001, pp.95–104.

[9] Y. Wu, D. Ma and R.H. Deng, "Progressive protection of JPEG 2000 codestreams," in *Proc. IEEE ICIP*, 2004, pp.3447–3450.

[10] Z. Zhang, Q. Sun, W.-C. Wong, J. Apostolopoulos, and S. Wee, "An optimized content-aware authentication scheme for streaming JPEG-2000 images over lossy networks," *IEEE Trans. Multimedia*, vol.9, pp.320–331, 2007.

[11] C.-L. Liu, "Layer stuffing tool for packet-based JPEG2000 image authentication," in *Proc. IEEE ISCE*, 2009, pp.67–70.

[12] J. Wen, J. Wang, F. Feng, and B. Zhang, "A reversible authentication scheme for JPEG2000 images," in *Proc. IEEE ICEMI*, 2009, pp.4-486–4-489.

[13] M. Palacios Perez, M. Fujiyoshi, and H. Kiya, "A codestream domain authentication and tamper localization scheme for JPEG 2000," in *Proc. IEEE ISCIT*, 2010, to be published.

[14] "Digital Cinema System Specification," ver.1.2, Digital Cinema Initiatives, LLC, 2008.

[15] X. Wang, Y.L. Yin, and H. Yu, "Finding collisions in the full SHA-1," in *LNCS*, vol.3621, 2005, pp.17–36.

[16] W. Trapple and L.C. Washington, "Introduction to cryptography with coding theory," Pearson Prentice Hall, 2006.

[17] "Advanced encryption standard," NIST FIPS 197, Nov. 2001. [Online]. Available: