Hash-based Identification of JPEG 2000 Images in Encrypted Domain

Toshiyuki DOBASHI*, Osamu WATANABE†, Takahiro FUKUHARA‡ and Hitoshi KIYA*
*Tokyo Metropolitan University, Dept. of Info. and Commun. Systems, 6–6 Asahigaoka, Hino-shi, Tokyo, JAPAN
†Takushoku University, Dept. of Electronics & Computer Systems, 815–1, Tatemachi, Hachioji-shi, Tokyo, JAPAN
‡Sony Corporation, CPDG PSG, 4–14–1, Asahi-cho, Atsugi-shi, Kanagawa, JAPAN

***Abstract*—A hash-based identification method for JPEG 2000 images is proposed in this paper. A new algorithm is introduced to calculate the hash value from the number of zero-bit-planes that can be extracted from the JPEG 2000 codestream by only parsing the header information. Furthermore, the proposed method uses hash value, and therefore, the length of the data used for identification is fixed. The processing speed of the proposed method should be fast since a fixed length data is used for the identification. The method avoids estimating an image from the feature because it uses hash value. Moreover, the image data can be encrypted because it uses pre-calculated hash value for identification. The experimental results showed the effectiveness of the proposed method.**

***Index Terms*—JPEG 2000, Image identification, Hash function, Digital Cinema, Encrypted Domain**

I. Introduction

The use of digital images and video sequences has greatly increased recently because of the rapid growth of the Internet and multimedia systems. It is often necessary to identify a certain image in a database that has a large number of digital images [1]–[6] in various types of the applications of digital images/videos. The image database generally consists of images in a compressed form to reduce the amount of data. Several international standards for searching still or moving images and retrieval systems have been developed [7]–[10] in connection to this. In this work, "identification" is defined as an operation for finding an image that is identical to a given original image from an image database.

JPEG 2000 [11] has been officially selected as the standard compression/decompression technology for digital cinema by the Digital Cinema Initiatives consortium [12]. There is need to identify a certain frame during some operations such as for the editing and re-encoding in digital cinema applications. The identification system used for digital cinema systems must be able to handle a large number of frames encoded by JPEG 2000 in a sufficiently short processing time. Several methods have been developed for identifying compressed images [1], [2], [5]. The method described in Ref. [1] is for JPEG images and uses the signs of the discrete cosine transform (DCT) coefficients of the images. One method for JPEG 2000 [2] uses the signs of the discrete wavelet transform (DWT) coefficients. An algorithm for both JPEG 2000 and JPEG was proposed in Ref. [5]. Although these methods are for compressed images, they use transformed coefficients, which are not available without decoding.

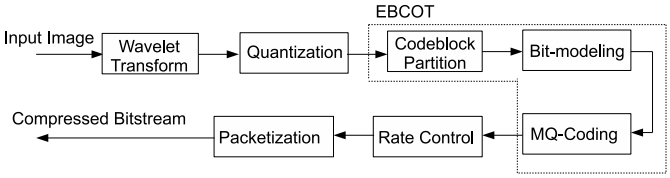

Fig. 1. Block diagram of JPEG 2000 encoder.

Codestream-based identification methods for JPEG 2000 images [3], [4], [13]–[15] have also been proposed. These methods achieve fast and precise image identification because they use the number of zero-bit-planes (NZBP), which is obtained by only parsing the header part of a JPEG 2000 codestream, as the features for the identification. Many of these methods purpose efficient identification, not secure identification. Several methods consider image encryption [13], but the feature data are not yet protected even in these methods.

Another problem is revealed that the length of feature, which is the number of zero-bit-planes, increases with an increase in the number of code-blocks. In digital cinema [12], a frame has a resolution of $4,000 \times 2,000$ and its JPEG 2000 codestream has over 20,000 code-blocks based on a typical code-block size. Thus, the length of a feature must be shortened for faster processing.

In this paper, a new algorithm for the calculation of hash value from the number of zero-bit-planes is introduced in order to process secure and fast identification, and a hash-based identification method for JPEG 2000 images is presented. The length of the feature data for identifying images for the proposed approach is fixed by using the hash value. The processing speed of the proposed approach should be fast because the length of a feature does not depend on the number of code-blocks. Moreover, not only are the image data encrypted but the also feature data are protected because the pre-calculated cryptographic hash value is used for the identification. The experimental results of an image identification based on the proposed approach are presented. The results revealed the effectiveness of the proposed method.

978-1-4673-5082-2 ©2012 IEEE

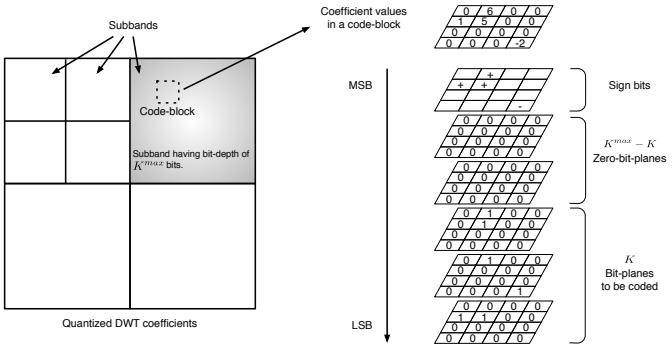

Fig. 2. Bit-plane decomposition and sign-magnitude representation of DWT coefficients in code-block. A zero-bit-plane is a special bit-plane in which the samples are all zeros. Zero-bit-planes are arranged from the MSB to the LSB level.

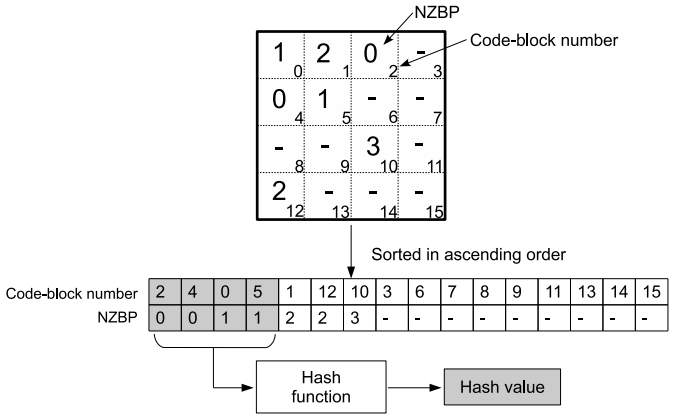

Fig. 3. Example of calculating hash value when $N = 4$. The dashed line represents the boundaries of the code-blocks. Symbol "-" means "not included."

II. Number of zero-bit-planes in JPEG 2000

A. Definition

Fig. 1 shows a block diagram of the JPEG 2000 encoder. JPEG 2000 uses a bit-plane coding architecture summarized as follows. As outlined in Fig. 2, quantized DWT coefficients are represented in sign-magnitude form. The sign bit-plane is at the MSB level, and the magnitude bit-planes are beneath it. The number of samples in a bit-plane is equal to that in the code-block, and all the samples in a bit-plane are either a 0 or 1. Let the K^{max} denote the number of bits required to represent all the quantized coefficients. The block coder for JPEG 2000 first determines the number of bits, $K \leq K^{max}$, that are needed to represent the quantized magnitudes. The encoder ideally finds the smallest such K. The difference between $K^{max} - K$ is called the "number of zero-bit-planes" and is defined as follows.

$$K^{msbs} = K^{max} - K \tag{1}$$

The NZBP, K^{msbs}, represents the number of most significant magnitude bits that is skipped to encode with the encoder. The decoder will take this to be zero for all samples. The remaining K magnitude bits must be explicitly coded. A code-block in which all the bit-planes are zero-bit-planes in the JPEG 2000 standard is defined as "not included" because the code-block does not contain any data to be encoded.

B. Effect of changes in coding rate on NZBP

Since the coding-rate in JPEG 2000 is normally controlled by discarding the MQ-encoded codestreams from LSB to MSB, it fundamentally has no effect on the NZBP even if the coding rate changes. However, the number of "not included" code-blocks may change if the coding rate changes. The NZBP is part of the header information of JPEG 2000 codestreams. This information is easily obtained by parsing the header part of JPEG 2000 without needing heavy EBCOT decoding.

III. Proposed method

A new identification method for JPEG 2000 images that uses hash value calculated by the number of zero-bit-planes is proposed in this section. Note that "Identification" in this work means an operation for finding an image that is identical to a given original image from an image database. However, the coding rates do not have to be same. Since the number of "not included" code-blocks may increase or decrease based on any change in the coding rate, if the NZBP of all the code-blocks are used for calculating the hash value, it would be sensitive to the coding rate. The proposed method uses only code-blocks that are less subject to the coding rate, not all the code-blocks. In other words, the proposed method does not use "not included" code-blocks. The procedure for calculating hash value in the proposed method is as follows.

Step1. The NZBP of all the code-blocks are extracted from the image.

Step2. The pair of the extracted NZBP and its code-block number is sorted in ascending order. The primary sort key is the NZBP and secondary one is the code-block number.

Step3. The first N pairs of the sorted pairs are brought together, and then, its hash value is calculated by using a cryptographic hash function.

The proposed method is based on the premise that the image has a certain number of code-blocks that are not "not included", and N is this number. The same N is applied to the query and database images. Fig. 3 shows an example of calculating the hash value when $N = 4$. This hash value is attached to JPEG 2000 image as extra information, and used for identification purposes. Thus, the image data can be encrypted and securely stored.

A. Hash-based identification

The hash value is calculated for and attached as extra information to a JPEG 2000 image. The image database is built with these hash-attached JPEG 2000 images. Let I^Q denote a query image and I^D denote a database image. Moreover, let H^Q denote the hash value for I^Q and H^D denote one for I^D.

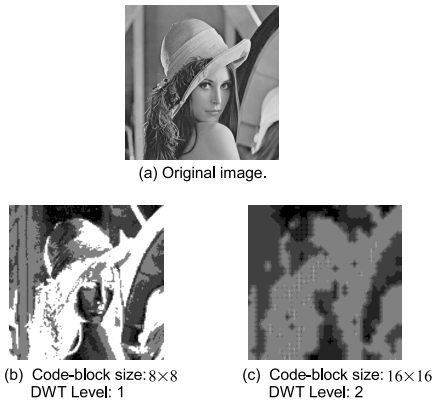

Fig. 4. Estimated images from NZBP.

Note that it is assumed that I^Q is also encoded as a JPEG 2000 image, and both hash values are calculated by using the proposed algorithm. An identification system based on the proposed algorithm returns a decision whether or not I^Q is identical to I^D. The decision D is made by using the following equations:

$$D = \begin{cases} Positive, & H^Q = H^D \\ Negative, & otherwise. \end{cases} \quad (2)$$

B. Image estimation from NZBP

The NZBP approximately represents the magnitude of the DWT coefficients. Thus, the DWT coefficients can be estimated from the NZBP, and the image can then be estimated. An estimated image from the NZBP is shown as Fig. 4. A conventional method [13] uses the NZBP directly for the identification, and thus, it can be estimated the image from the feature, i.e., insecure. By contrast, the proposed method does not allow an adversary to estimate the image from the feature because the hash value is used for the identification.

IV. Experimental results

The performances of the identification methods were evaluated in terms of their precision and processing speed of the image identification to verify the effectiveness of the proposed method.

A. Conditions and Procedure

The Standard Evaluation Material (StEM) [16] was used as the test sets. The test sequence contained 8,927 frames. The specifications for the test sequences are summarized in Table I.

First, the sequences of the JPEG 2000 compressed images were built for database of hash values. The encoding parameters for the sequences are listed in Table II. Kakadu [17] version 6.4 was used as the JPEG 2000 codec. The hash values for all the encoded frames in the sequences were calculated by using the proposed algorithm offline and the calculated hash values were stored into the database. The hash value for a query image was calculated followed by the JPEG 2000 encoding with the coding parameters for a query listed in Table II. Note that the coding rate for a query was different from that for the database.

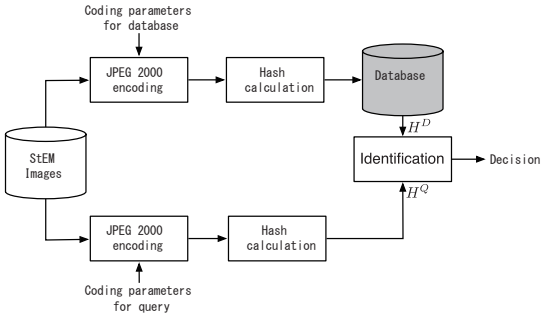

Fig. 5. Procedure used in identification experiment.

TABLE I
Specifications for standard evaluation material [16].

No. of frames	8,927
Spatial resolution	4,096 (H)× 1,740 (V)
Color format	RGB (4:4:4) 12 bits/component

Identificaion experiments were carried out for all the possible combinations of the frames to verify that the proposed method correctly identifies the compressed frames with different coding rates. There were 8,927×8,927 combinations. In JPEG 2000, the color space is usually converted to YC_bC_r for effective compression. In this experiment, only component Y was used for calculating the hash value because component C_b and C_r have many "not included" code-blocks. Component Y contained 6,992 code-blocks. Parameter N for calculating the hash value was set to 699, 1398, 2097, 2796, and 3496, which corresponded to 10%, 20%, 30%, 40%, and 50% of the number of code-blocks, respectively. Fig. 5 outlines the procedure for these experiments.

B. Results and remarks

(A) Performance of identification: The number of true-positive (TP), true-negative (TN), false-positive (FP), and false-negative (FN) decisions obtained from the experiment are listed in Tab. III. This table also notes the false-positive-rate (FPR) and true-positive-rate (TPR) [18] with the results. A receiver operating characteristic (ROC) curve [18] built with the FPRs and the TPRs is shown in Fig. 6. The ROC

TABLE II
JPEG 2000 encoding parameters.

Codec	Kakadu version 6.4
DWT Filter	9×7
DWT Level	5
Coding rate (VBR)	237.6 Mbps (for query)
	136.0 Mbps (for database)
Code-block size	32×32
Color space	YC_bC_r
Tile decomposition	No

TABLE III
NO. OF TRUE-POSITIVE (TP), TRUE-NEGATIVE (TN), FALSE-POSITIVE (FP), AND FALSE-NEGATIVE (FN) RESULTS OBTAINED FROM EXPERIMENT.

N	TP	TN	FP	FN	FPR(%)	TPR(%)
699	8754	79671388	11014	173	0.014	98.1
1398	8701	79672006	10396	226	0.013	97.5
2097	8640	79672662	9740	287	0.012	96.8
2796	8430	79672754	9648	497	0.012	94.4
3496	8143	79674568	7834	784	0.009	91.2

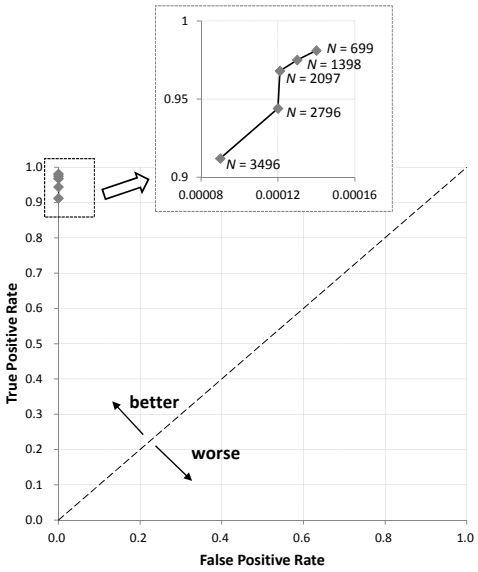

Fig. 6. ROC curve of identification experiments. Each point was depicted with the FPR and TPR values in Tab. III. The dashed-line in the figure represents the performance of a random guess.

curve depicts the relative trade-offs between the benefits (true-positives) and costs (false-positives). Informally, one point in ROC space is better than another if it is northwest (TPR is higher, FPR is lower, or both) of the first.

The points depicted with the results of Tab. III are all in the "better" area. Therefore, it can be verified that identification based on the proposed method could identify the query frames regardless of the difference in the coding rate.

(B) Complexity of Identification: The conventional method [13] uses the NZBP itself as the feature for image identification, and the length of the feature data depends on the total number of code-blocks in a JPEG 2000 codestream. If the size of the image becomes large, the number of code-blocks will increase. For example, for 32×32 sized code-blocks, there are over 20,000 code-blocks for an image with a resolution of $4,000 \times 2,000$.

By contrast, the proposed method does not directly use the NZBP. By using a cryptographic hash function, the length of the feature is fixed. For example, for the MD5 hash function, the length of the feature is 128 bit. Clearly, the complexity of the proposed method is relatively smaller than that of the conventional method.

V. CONCLUSION

A hash-based identification method for JPEG 2000 images has been presented in this paper. A new algorithm for installing a hash function into codestream-based identification has been described. The proposed method correctly identifies the JPEG 2000 codestreams even if there is a difference in the coding rates. The length of feature is fixed by using the hash value. In most cases, the length of the feature is shorter than that of the conventional method. Moreover, the method does not allow an adversary to estimate the image from the feature because using hash value. The image data can also be protected by being encrypted and securely stored since pre-calculated hash value is used for identification.

ACKNOWLEDGMENT

This work has been partially supported by the Grand-in-Aid for Scientific Research (C), No.16500066, from the Japan Society for the Promotion of Science.

REFERENCES

[1] F. Arnia, I. Iizuka, M. Fujiyoshi and H. Kiya, "Fast and Robust Indentification Methods for JPEG Images with Various Compression Ratios," in *Proc. ICASSP 2006*, vol. 2, no. IMDSP-P.4.6, May 2006, pp. 397–400.
[2] O. Watanabe, A. Kawana and H. Kiya, "An Identification Method for JPEG2000 Images Using the Signs of DWT Coefficients," *Technical Report of IEICE*, vol. 106, no. IE2006-217, pp. 177–181, Jan. 2007.
[3] T. Fukuhara, K. Hosaka and H. Kiya, "Accurate identifying method of JPEG2000 images for digita cinema," in *Proceedings of The 14th International Multimedia Modeling Conference (MMM'08)*, vol. 4903. Lecture Notes in Computer Science, Jan. 2008, pp. pp.380–390.
[4] T. Fukuhara, K. Hosaka and H. Kiya, "Identifying method of JPEG2000 images in the codestream level for digital cinema (in Japanese)," *IEICE Trans.*, vol. J91-D, no. 9, pp. 2305–2313, 2008.
[5] K. O. Cheng, N. F. Law, W. C. Siu, "A fast approach for identifying similar features in retrieval of JPEG and JPEG 2000 images," in *Proc. APSIPA ASC 2009*, no. MP-P2-3, Oct. 2009.
[6] Y. Uchida and S. Sakazawa, "Near-Duplicate Video Detection Considering Temporal Burstiness of Local Features," in *Proc. The 2011 IEICE General Conference*, no. D-12-93, Mar. 2011 (in Japanese), p. 196.
[7] "Information technology – JPSearch – Part 1: System framework and components," International Standard ISO/IEC TR-24800-1, Dec. 2007.
[8] "Compact Descriptors for Visual Search: Applications and Use Scenarios," ISO/IEC JTC1/SC29/WG11/N11529, Jul. 2010.
[9] "Compact Descriptors for Visual Search: Context and Objectives," ISO/IEC JTC1/SC29/WG11/N11530, Jul. 2010.
[10] "Compact Descriptors for Visual Search: Requirements," ISO/IEC JTC1/SC29/WG11/N11531, Jul. 2010.
[11] "Information technology — JPEG 2000 image coding system – Part 1: Core coding system," International Standard ISO/IEC IS-15444-1, Dec. 2000.
[12] "Digital Cinema System Specification V1.2," Digital Cinema Initiatives, LLC Technology Committee, Mar. 2008.
[13] O. Watanabe, T. Iida, T. Fukuhara and H. Kiya, "Identification of JPEG 2000 images in encrypted domain for Digital Cinema," in *Proc. of IEEE ICIP*, vol. 2, no. MA.PJ.8. IEEE, Nov. 2009, pp. 2065–2068.
[14] O. Watanabe, T. Fukuhara and H. Kiya, "Fast Identification of JPEG 2000 Images for Digital Cinema Profiles," in *Proc. ICASSP 2011*, May 2011, pp. 881–884.
[15] O. Watanabe, T. Fukuhara and H. Kiya, "Codestream-Based Identification of JPEG 2000 Images with Different Coding Parameters," *IEICE Transactions on Information and Systems*, vol. E95-D, no. 4, pp. 1120–1129, 2012.
[16] Digital Cinema Initiatives, LLC Technology Committee, "StEM Access Procedures," http://www.dcimovies.com/StEM/, Sep. 2010.
[17] "Kakadu software," http://www.kakadusoftware.com/.
[18] T. Fawcett, "An introduction to roc analysis," *Pattern Recognition Letters*, vol. 27, no. 8, pp. 861 – 874, 2006.