IDENTIFICATION OF JPEG 2000 IMAGES IN ENCRYPTED DOMAIN FOR DIGITAL CINEMA

Osamu WATANABE†, Tomonori IIDA‡, Takahiro FUKUHARA , and Hitoshi KIYA‡*

†Takushoku University, Dpet. of Electronics & Computer Systems, 815–1, Tatemachi, Hachioji-shi, Tokyo, JAPAN
‡Tokyo Metropolitan University, Dept. of Info. and Commun. Systems Eng., 6–6 Asahigaoka, Hino-shi, Tokyo, JAPAN
* Sony Corporation, B2B Solution Dept., 4–14–1, Asahi-cho, Atsugi-shi, Kanagawa, JAPAN

ABSTRACT

A bit-stream-level method for identifying encrypted JPEG 2000 images without having to decrypt them is described. It is well known that editing the scenes of the movie is often necessary. In the editing process, image identification plays an important role in finding a frame that should be re-encoded. Thus, identification of encrypted images is very useful in digital cinema because all frames in digital cinema are encoded and encrypted. The proposed method directly uses encrypted JPEG 2000 images so that decryption-free identification without JPEG 2000 decoding is possible. The proposed method is both accurate and fast. In principle, identification based on the proposed method does not produce false negative matches regardless of the compression ratio. Moreover, since there is no need to decode and decrypt the images, the average processing time for identification is very short and independent of the encoded image size.

Index Terms— JPEG 2000, JPEG 2000 search, Image identification, Digital Cinema

1. INTRODUCTION

Media security has become a serious problem because the exchange multimedia data (e.g., images, and movies) via public networks (e.g., the Internet) has become very common. The data is usually encrypted due to copyright and/or privacy concerns. However, there is a growing demand for the ability to process media data without having to decrypt it. Several studies related to this problem have been presented for imaging applications [1–4]. Since digital images are mostly coded by using an image compression scheme such as JPEG, for a system to be practical, the intended processing should not require decoding and decryption procedures.

It is often necessary to identify media data in a database that has a large amount of digital content, and several methods have been developed for identifying images [5–7]. Two [5, 6], for example, are for JPEG images and use the signs of the discrete cosine transform (DCT) coefficients. One for JPEG 2000 [7], uses the signs of the discrete wavelet transform (DWT) coefficients. Although these methods are for compressed images, they use transformed coefficients, which are not available without decoding. A code-stream-based identification method for JPEG 2000 images [8], which does not handle encrypted images, features fast identification. JPEG 2000 was officially selected as the standard compression/decompression technology for digital cinema by the DCI (Digital Cinema Initiatives) consortium [9], and standards for identifying and retrieving JPEG 2000 images are now being developed [10]. The identification system used for digital cinema systems must be able to handle a very large number of JPEG 2000-encoded frames in a sufficiently short processing time.

The method presented in this paper achieves JPEG 2000 image identification without decryption and decoding. Identification is defined as an operation for finding from an image that is identical to a given original image among JPEG 2000 encoded images. The coding rates of the encoded images are not necessarily identical. The processing time for identification is very short because the information is obtained by parsing only the header and using a previously reported method [8]. Any encryption method that does not affect the zero-bit-plane information can be used with the proposed method.

This paper is organized as follows. In section 2, the JPEG 2000 coding system is described. The proposed method is described in section 3. In section 4, experimental results are presented showing that the proposed method achieves very fast, accurate, and robust identification. Section 5 concludes the paper with a brief summary.

2. FEATURE OF JPEG 2000 TECHNOLOGY

In this section, the fundamental technology of JPEG 2000 is described, because the proposed method effectively takes advantage of JPEG 2000 codestream.

2.1. Basic Technology

Fig.1 is a block diagram of JPEG 2000 encoder. Wavelet transform analyzes input image and generates subband domains which are groups of wavelet coefficients. Wavelet coefficients in subband domains are quantized to generate quantized coefficients. Quantized coefficients are grouped in codeblocks. Value of the coefficients is represented as the bit-plane of sign and absolute value(Fig.2). EBCOT is an unique entropy coder of JPEG 2000 and generates compressed codestream by the combination of bit-modeling and MQ coding(arithmetic coding). In rate control, some coding-passes are truncated so as to adjust the amount of the codestream within the target size. In the last part of encoder, an incremental packet header is added to the codestream to generate JPEG 2000 compliant codestream.

2.2. Bit-Plane

JPEG 2000 adopts the technology of bit-plane which is completely different from the other compression technologies such as JPEG and MPEG. Quantized coefficients are represented in three dimensions; horizontal, vertical and bit-depth. There are the same number of bit-planes as the number of the bit-depth from MSB(Most Significant Bit) to LSB(Least Significant Bit). Each bit-plane contains the number of samples in a codeblock. All of the samples in bit-plane are either 0 or 1. Fig.2 is an example of codeblock with 16 samples(4 rows x 4 lines). zero-bit-plane is a special bit-plane whose samples are all zeros. Zero- bit-planes are located from MSB to lower significant direction. Bit-Planes except zero- bit-planes are the object of encoding and decoding. Four examples of zero-bit-plane are shown in Fig.3. The number of zero-bit-planes in the first codeblock(left-hand side)

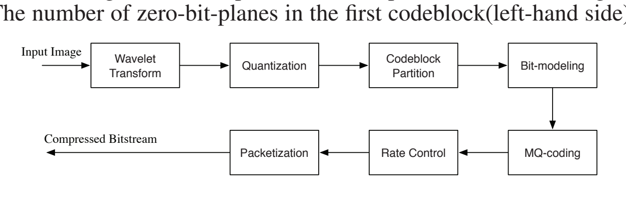

Fig. 1. Block diagram of JPEG 2000 encoder

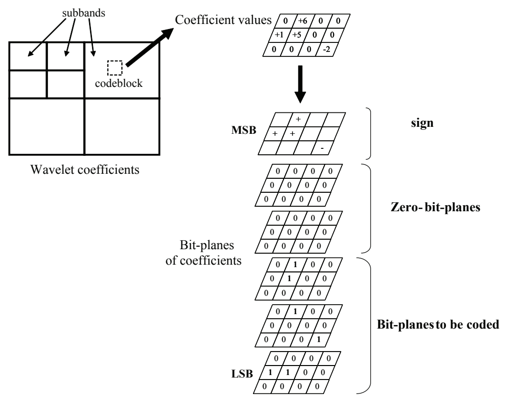

Fig. 2. Code Blocks and bit-planes: Zero-bit-plane is a special bit-plane in which samples are all zeros. Zero- bit-planes are arranged from MSB level to LSB level.

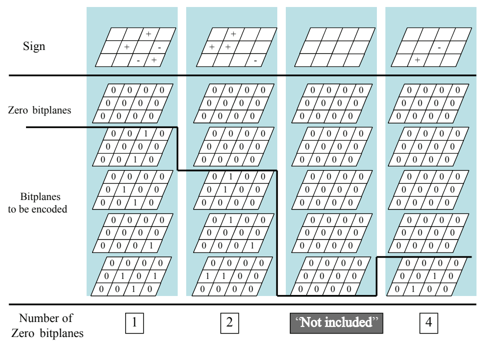

Fig. 3. Number of zero-bit-plane and "Not included"

equals to one, because the only MSB bit-plane is zero-bit-plane. In the same manner, the number of zero-bit-planes in the second one and the fourth one(right-hand side) are two and four respectively. But the third codeblock should be taken care, because all of the bit-planes are zero-bit-planes. In JPEG 2000 standard, this codeblock is defined as "not included", because the codeblock does not have any data to be encoded. Since the rate-control in J2 is normally achieved by discarding the MQ-encoded codestreams from LSB toward MSB, there is fundamentally no influence in the number of zero-bit-planes even if the coding-rate changes.

2.3. Structure of JPEG 2000 bitstream

JPEG 2000 bitstream consists of more than one packet. A packet has a packet-header and a packet body, and the information of each codeblock which belongs to the packet, the number of coding-pass and the number of zero-bit-plane, and so on, are stored in the packet-header of JPEG 2000 codestream. Therefore, the number of zero-bit-plane in a codeblock can be obtained by only parsing the packet-header.

3. PROPOSED METHOD

In this section, firstly, the supposed use-case of proposed method is explained. Secondly,the procedures of the identification and encryption are summarized, then the structure of the proposed identification for encrypted images is described.

3.1. Problem setup

As shown in Fig.4, the image identification based on the image database composed of encrypted JPEG 2000 images is assumed in

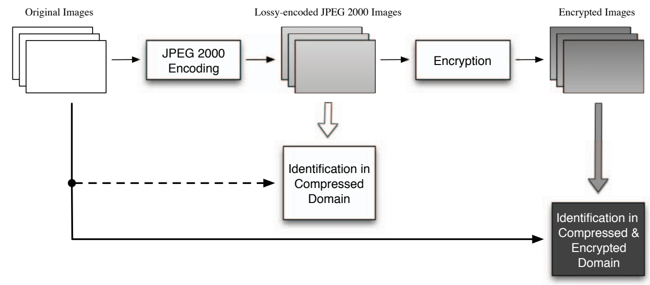

Fig. 4. Model of image identification: dashed line and solid line is equal to the conventional method and the proposed method, respectively.

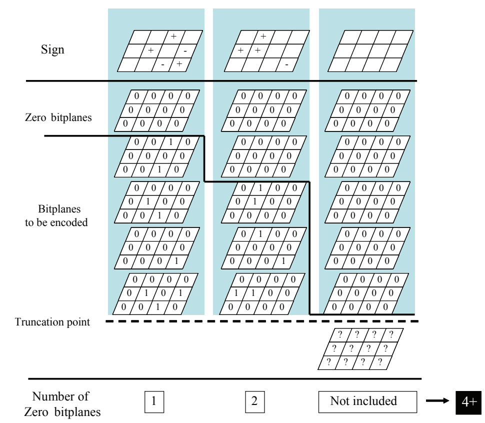

Fig. 5. Re-definition of number of zero-bit-planes:The third codeblock is re-defined as "4+", instead of "not included". It is because 4 zero-bit-planes actually exist. But if there were non-zero-bit-planes before truncation in the LSB direction, the number of bit-planes would be 4 or more.

this paper. For example of this kind of database, image sequences such as movies are commonly considered. In applications like digital cinema, images in the image database are generally encoded with the identical coding parameters (image size, number of DWT, codeblock size, presence of tiles, and so on). Therefore, we assume the condition that all images in the encrypted image database are encoded with the identical coding parameters. From the image database, the proposed method identifies the images which have the same original image as the query.

3.2. Identification method

3.2.1. Re-definition of number of zero-bit-planes

The method in [8] identifies between query image(image-A) and database(image-B) images with the following decision criteria. In order to increase the success rate of identification when either image-A or image-B has "not included" codeblock, the number of bit-plane is used. The third codeblock in Fig.5 is defined as "4+", instead of "not included" in Fig. 3. It is because 4 zero-bit-planes actually exist in the codeblock. But if there were non-zero-bit-planes before truncation in the LSB direction, the number of zero-bit-planes would be 4 or more.

3.2.2. Decision criteria

- **Rule-0:** Identification of image is successful if all codeblocks of image-A and image-B are determined as "the same" based on following rules(Rule-1, 2, 3).

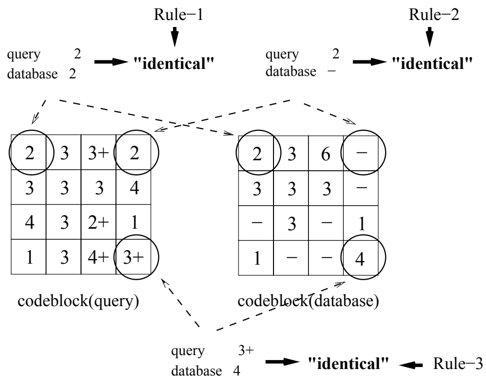

Fig. 6. Rules of codeblock identification("Not included" in query is transformed to $K+$)

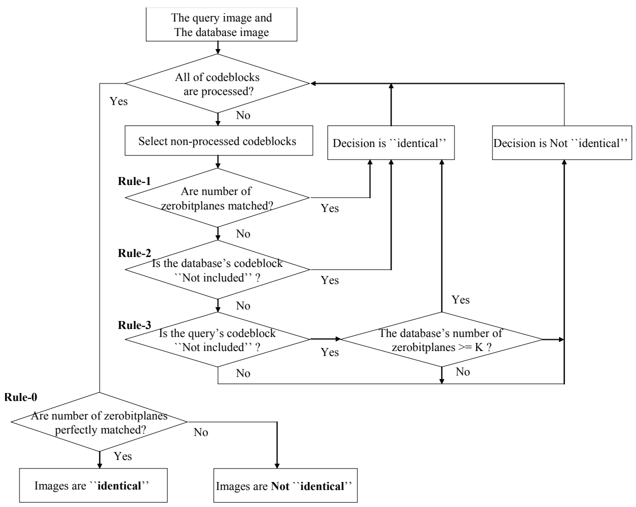

Fig. 7. Procedure of identification for encrypted JPEG 2000 images.

- **Rule-1:** Identification is successful if the number of all zero-bit-planes in the same position of codeblocks of image-A and image-B are perfectly the same.
- **Rule-2:** If a codeblock of image-B is "not included", identification is success regardless of the number of bit-plane of image-A.
- **Rule-3:**If a codeblock of image-A is "not included", the number of zero-bit-planes is counted. If the number is "K", it is defined as "K+". If the number of zero-bit-plane of image-B is equal to or more than "K", they are identified as the same. According to the above rule, "4+" of image-A is identified as the same as "5" of image-B. Fig. 6 shows the examples of the identification process.

Fig.7 shows the example of the above procedure.

3.3. Encryption of JPEG 2000

There are some methods for encryption of JPEG 2000 images. Generally, these methods are classified into following three types.

- (Type-1) Encrypting the data under encoding process [11]
- (Type-2) Partial encryption of JPEG 2000 bitstream [12]
- (Type-3) Encryption of entire JPEG 2000 file

The methods categorized into Type-1 encrypt the data under encoding process, such as the quantized coefficients. For example, the sign of quantized DWT coefficients are inverted in [11]. Type-2 methods encrypt only the body data of generated JPEG 2000 bitstream. This encryption is performed after entire encoding process. Type-3 methods are equal to mere file encryption and the packet-header is of-course encrypted. Therefore, the number of bit-plane is no longer available without decryption of entire file.

Partial encryption of body data by Type-1 or Type-2 methods makes it possible that partially encrypted JPEG 2000 bitstreams are recognized as image , so that decoded JPEG 2000 images can be visualized without any decryption. For this reason, encryption methods in Type-1 or Type-2 are supposed to use in the proposed method.

3.4. Identification from encrypted JPEG 2000 images

It is assumed that the database JPEG 2000 images are encrypted and the identification process will be performed to these encrypted images. The query image is the original image(not encoded) of the JPEG 2000 image to be identified in the database. The identification processes are summarized as follows:

- (Step-1) Coding-parameters(DWT Level, Quantization step size, size of codeblock, etc) are extracted from the database images.
- (Step-2) The query image is encoded by using the extracted coding-parameters.
- (Step-3) Identification processing described on section 3.2 are performed between the encoded query image obtained in Step-2 and the encrypted database images.

The necessary parameters for JPEG 2000 encoding are extracted from the database images in Step-1. Because the database images are encoded by using DCI compliant JPEG 2000 standard, all of them have the same coding-parameters. However, coding-rate of each image is not identical because VBR(Variable Bit Rate) is adopted in DCI standard.

In Step-2, the query image is encoded by JPEG 2000 with the extracted coding-parameters. Since the database images are encoded by identical parameters, this encoding is necessary only once.

The identification processing are performed between the encoded query image and the encrypted database images in Step-3. Provided that one of methods explained in 3.3 is used, decryption is not necessary to parse the packet header. Therefore the number of zero bit-plane is obtained without any decryption and the identification process described in 3.2 can be applied for encrypted images with no modification.

4. EXPERIMENTS AND RESULTS

In this section, the performance of the identification is demonstrated to verify the effectiveness of the proposed method. Firstly, sequence of JPEG 2000 compressed images are stored in database. A query image is searched and identified out of the JPEG 2000 images in database.

4.1. Experimental Condition

In the experiment, the StEM(Standard Evaluation Test Material) is used. The number of test frames is 14,989(there are more original frames in StEM, but those images with visually full black-color are rejected from the test sequence). The resolution is $4,096 \times 1,714$, which is about four times as large as full-HDTV. Encoding condition is shown in Table1. Note that the test sequences are encoded at four different bit-rates.

4.2. Experimental results

4.2.1. Accuracy

The False-Positive(FP) rate of all trial for the identification is shown in Fig.8. This rate is calculated by following equation.

$$FPrate = nFP/N \quad (1)$$

Table 1. Test sequence and JPEG 2000 encoding condition

Test sequence	StEM (DCI standard), 14,981 frames
Resolution	4,096 (Horizontal) × 1,740 (Vertical)
Format	RGB (4:4:4) 12 bits/component
Average bit-rate [Mbps]	388, 304, 224, 171, 146, 100, 77, 51, 24
Rate control	VBR (variable bit rate)
Encoding parameters	DCI Compliant (JPEG 2000 Part-1) DWT decomposition level = 5 Code block size = 32 × 32 Precinct size = 256 × 256 (LL=128 × 128) No tile decomposition

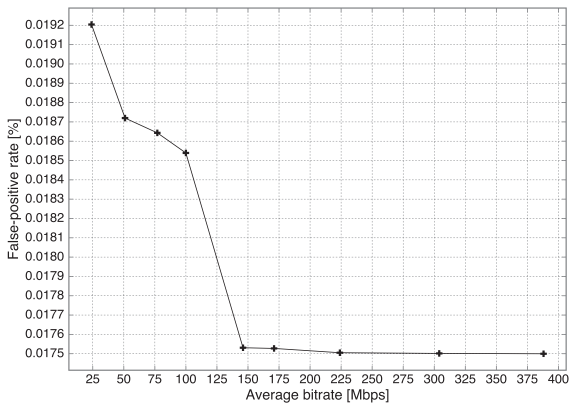

Fig. 8. False-positive rate: calculated using equation(1).

where nFP and N mean the number of FP frames and the number of all possible combination of the query and the database($= 14989 \times (14989 - 1)$), respectively. From Fig.8, it is shown that the false-positive-rate of the the proposed method is about only 0.0175% in every coding-rate.

Figure 9 shows the index of dissimilarity. The dissimilarity which is obtained by summation of the difference of the number of zero-bit-planes between the query and the database image is shown by the vertical axis. The horizontal axis means the frame number of the database image. In this experiment, the 2750th frame has been used as the query. Clearly the dissimilarity at the 2750th frame is zero so that it is shown that the proposed method correctly identified the image that has the same original image as the query.

4.2.2. *Speed*

The average processing time of the proposed method is about 0.6[ms/frame](without disk access time). Because there are no need to decrypt/ decode encrypted JPEG 2000 images, the proposed identification is performed very fast regardless of the bit rate.

5. CONCLUSIONS

In this paper, a bitstream level identification method for encrypted JPEG 2000 images without decryption has been proposed. Some experimental results on identification of DCI based JPEG 2000 images has been provided to evaluate the performance of the proposed method. It has been shown that the identification based on the proposed method never produce false positive matches regardless of the compression ratio and averaged time consumption is very small and is not dependent on encoded image size.

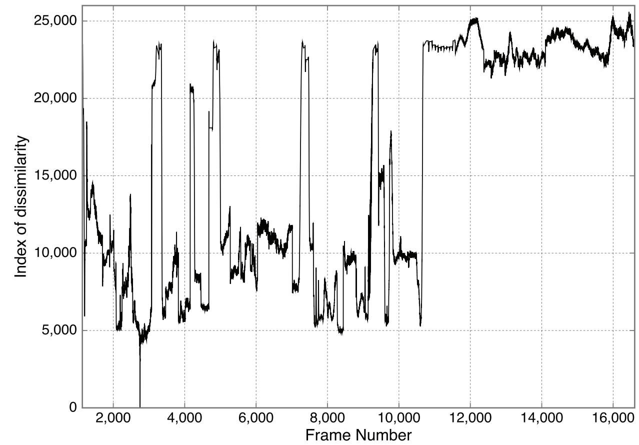

Fig. 9. Index of dissimilarity when 2750th frame was used as query image. The zero dissimilarity at 2750th frame shows that proposed method correctly identified database image matching query image.

6. REFERENCES

[1] A.K. Jain, A. Ross and S. Pankanti, "Biometrics: A Tool for Information Security," *IEEE Trans. on Inf. Forensics Security*, vol. 1, no. 2, pp. 125–143, jun 2006.

[2] K. Kuroiwa, M. Fujiyoshi and H. Kiya, "Codestream Domain Scrambling of Moving Objects Based on DCT Sign-Only Correlation for Motion JPEG Movies," *IEEE ICIP*, vol. V, pp. 157–160, sep 2007.

[3] T. Bianchi, A. Piva and M. Barni, "Implementing the Discrete Fourier Transform in the Encrypted Domain," *IEEE ICASSP*, pp. 1757–1760, 2008.

[4] I. Ito and H. Kiya, "A New Class of Image Registration for Guaranteeing Secure Data Management," *IEEE ICIP*, , no. MA-PA.5, pp. 269–272, oct 2008.

[5] F. Arnia, I. Iizuka, M. Fujiyoshi and H. Kiya, "Fast and robust indentification methods for jpeg images with various compression ratios," in *Proc. of ICASSP 2006*. IEEE, May 2006.

[6] Fitri Arnia, I. Iizuka, M. Fujiyoshi, and H. Kiya, "Fast image identification methods for jpeg images with differe nt compression ratios," *IEICE trans. Fundamentals*, vol. E89-A, no. 6, pp. 1585–1593, June 2006.

[7] 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.

[8] T. Fukuhara, K. Hosaka and H. Kiya, "Accurate identifying method of JPEG2000 images for digital cinema," in *Proc. of The 14th International Multimedia Modeling Conference*. Lecture Notes in Computer Science, Jan. 2008, vol. 4903.

[9] "Digital Cinema System Specification V1.0, Final approval," Digital Cinema Initiatives, LLC Technology Committee, July 2005.

[10] "JPSearch Part1 Technical Report(Type3): ISO/IEC PDTR 24800-1 Framework and System Components," JPSearch AHG , 2006 Nov.

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

[12] S. Imaizumi, O. Watanabe, M. Fujiyoshi and H. Kiya, "Generalized Hierarchical Encryption of JPEG 2000 Codestreams for Access Control," *IEEE ICIP*, vol. II, pp. 1094–1097, sep 2005.