INTEGRITY AUTHENTICATION METHOD FOR JPEG IMAGES USING REVERSIBLE WATERMARKING

Hyun-Wu Jo, Dong-Gyu Yeo and Hae-Yeoun Lee
Dept. of Computer Software Engineering, Kumoh National Institute of Technology, Sanho-ro 77, Gumi, Gyeongbuk 730-701, Korea

Keywords: Image Authentication, JPEG Compression, Reversible Watermark, DCT Coefficient.

Abstract: In these days, with increasing the importance of multimedia security, various multimedia security techniques are studied. In this paper, we propose a content authentication algorithm based on reversible watermarking which supports JPEG compression commonly used for multimedia contents. After splitting image blocks, a specific authentication code for each block is extracted and embedded into the quantized coefficients on JPEG compression which are preserved against lossy processing. At a decoding process, the watermarked JPEG image is authenticated by extracting the embedded code and restored to have the original image quality. To evaluate the performance of the proposed algorithm, we analyzed image quality and compression ratio on various test images. The average PSNR value and compression ratio of the watermarked JPEG image were 33.13dB and 90.65%, respectively, whose difference with the standard JPEG compression were 2.44dB and 1.62%.

1 INTRODUCTION

Multimedia contents can be copied and manipulated without quality degradation. Therefore, they are vulnerable to digital forgery and illegal distribution. In these days, with increasing the importance of multimedia security, various multi-media security techniques are studied.

Digital watermarking can be an efficient solution to protect multimedia security and digital right management, which inserts confidential information called as the watermark into multimedia contents themselves. By retrieving the inserted watermark from the contents, it can be used for various purposes including ownership verification, copyright protection, broadcast monitoring, and contents authentication, etc.

In this paper, we propose a content authentication algorithm based on reversible watermarking which supports JPEG compression commonly used for multimedia contents. After splitting image blocks, a specific authentication code for each block is ex-tracted and embedded into the quantized coefficients on JPEG compression. At a decoding process, the watermarked JPEG image is authenticated by ex-tracting the embedded code and restored to have the original image quality.

The paper is composed of as follows. In Sec. 2, related researches are summarized. We present image authentication algorithm for JPEG compression in Sec. 3. Experimental results are shown in Sec. 4 and Sec. 5 concludes.

2 RELATED WORKS

The purpose of image authentication is to detect tempering and to prove the integrity of the image. In the various types of watermarking algorithms, fragile watermarking is easily corrupted by slightest modification and applicable for this purpose.

Yuan and Zhang proposed a fragile watermarking method for image authentication based on statistical analysis in the wavelet (Yuan, 2003). Hu and Han suggested a semi-fragile watermarking algorithm for image authentication (Hu, 2005), in which image features are extracted from the low frequency domain to generate two watermarks. One feature is used to classify the intentional content modification and the other is used to indicate the modified location. A compressed-domain fragile watermarking scheme with discrimination of tampers on image content or watermark was studied (Wang, 2009).

Li proposed a transform-domain fragile

Jo H., Yeo D. and Lee H..
INTEGRITY AUTHENTICATION METHOD FOR JPEG IMAGES USING REVERSIBLE WATERMARKING.
DOI: 10.5220/0003826200830086
In *Proceedings of the International Conference on Computer Vision Theory and Applications* (VISAPP-2012), pages 83-86
ISBN: 978-989-8565-04-4

watermarking algorithm for authentication. However, this method uses a private key to generate binary-sequence therefore it needs to share a private key between sender and receiver. Furthermore, this method doesn't consider about reversibility of algorithm (Li, 2004).

In most previous researches, uncompressed images were considered and the quality of the original image was degraded although it was not perceptible to human eyes. Also, they were vulnerable against JPEG compression since the JPEG compression could be considered as a kind of attacks.

3 PROPOSED ALGORITHM

JPEG compression is a commonly used compression standard for images. Therefore, the way to check the integrity and ensure the original quality of JPEG compressed images should be provided. In this section, we present a JPEG image authentication algorithm based on reversible watermarking which is composed of two parts: insertion and authentication. At the insertion process, the authentication code is generated using the characteristics of an image block and inserted into image data itself during the JPEG compression process. At the authentication process, the embedded watermark is extracted and used to prove the integrity. Also, the original quality is ensured by removing the embedded watermark.

3.1 Watermark Insertion

The overall process to insert watermark is depicted on Fig. 1. Input image goes through lossy processing step and lossless processing step on JPEG compression. Quantized DCT (QDCT) blocks from discrete cosine transform and quantization at the lossy processing step do not make loss in the entropy coding progress. Therefore, we insert the authentication code (called the watermark) into this QDCT blocks in a reversible way because they are preserved against image compression.

The authentication code is generated as follows (refer Fig. 2):

- Make a 8x8 grayscale block through down-sampling a 16x16 color block
- Apply DCT to 8x8 grayscale block and quantize DCT coefficients
- Extract most significant 8 values from quantized DCT coefficients in Zigzag order, which is the 64 bits authentication code

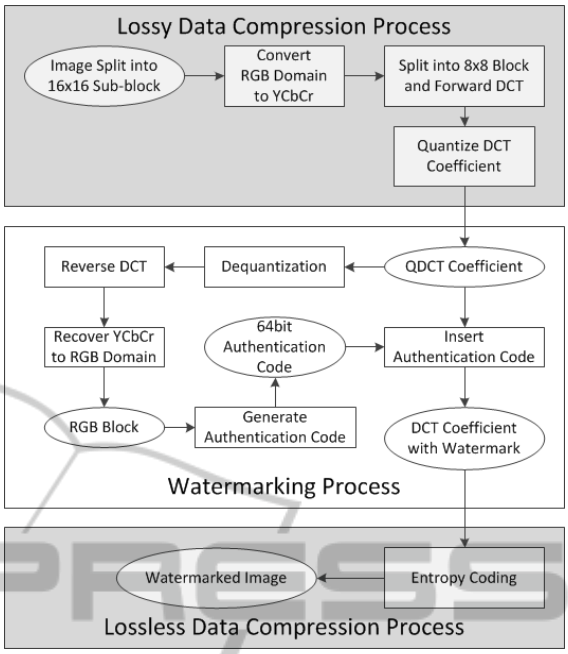

Figure 1: Overall watermark insertion process.

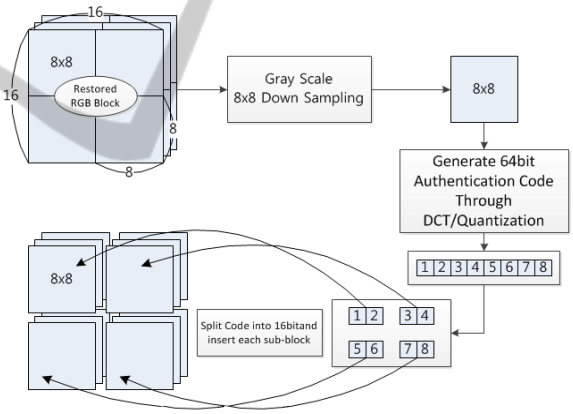

Figure 2: Authentication code generation and splitting.

As shown in Fig. 2, the 64 bits authentication code is split into four 16 bits sub-codes and inserted into each 8x8 sub-blocks. One block is composed by 3 channels: Y, Cb, Cr. The 16 bits sub-code is split again into 8, 4, and 4 bits to be inserted into each channel.

The way to insert this authentication code is based on histogram shifting for DCT coefficients as shown in Fig. 3. We insert the authentication code by shifting the zero value in DCT coefficients. Usually, modifying the DC coefficient has effects on quality degradation over other coefficients and its possibility to have zero value is very low. Therefore, Except the DC coefficient, the insertion proceeds from most significant coefficients to least significant

coefficients in zigzag order.

This watermark insertion using histogram shifting can be formulated as equation (1). ZQDCT is Zigzag-reordered QDCT Coefficient.

$$ZQDCT\omega_{(i)} = \begin{cases} ZQDCT_{(i)}, & if\ i = 0 \\ ZQDCT_{(i)}, & if\ ZQDCT_{(i)} < 0 \\ ZQDCT_{(i)} + 1, & if\ ZQDCT_{(i)} > 0 \\ ZQDCT_{(i)} + wm_{(j)}, & if\ ZQDCT_{(i)} = 0 \end{cases} \quad (1)$$
$$for\ 0 \le j \le (sizeof(watermark) - 1),$$
$$i = index\ of\ Zig - zag\ reordering$$

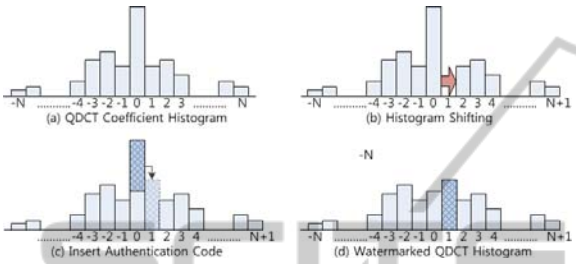

Figure 3: Histogram shifting for watermarking.

3.2 Image Authentication

The overall process to authenticate images and restore the original quality is depicted on Fig. 4. The main idea of image authentication and tamper detection is originated from the characteristic of JPEG compression method.

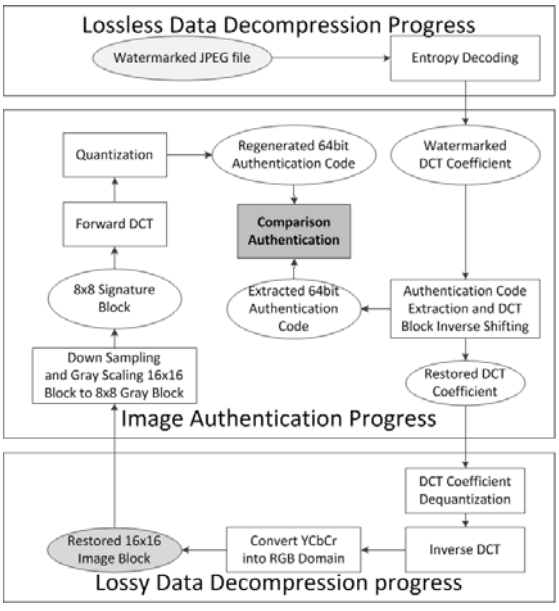

Figure 4: Overall image authentication process.

The authentication code is regenerated by using the same steps in the watermark insertion. The way to extract the watermark and to restore the original quality is depicted in Fig. 5 and can be modelled as equation (2) and (3).

$$wm_{(j)} = \begin{cases} skip, & if\ i = 0 \\ ZQDCT\omega_{(i)}, & if\ ZQDCTw_{(i)} \in \{0,1\} \end{cases} \quad (2)$$
$$for\ 0 \le j \le (sizeof(watermark) - 1),$$
$$i = index\ of\ Zig - zag\ reordering$$

$$ZQDCT\omega_{(i)} = \begin{cases} ZQDCT\omega_{(i)}, if\ i = 0 \\ ZQDCT\omega_{(i)}, if\ ZQDCT\omega_{(i)} < 0 \\ ZQDCT\omega_{(i)} - 1, if\ ZQDCT\omega_{(i)} > 0 \end{cases} \quad (3)$$
$$for\ i = index\ of\ Zig - zag\ reordering$$

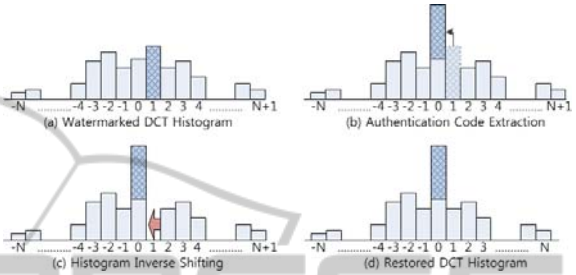

Figure 5: Image restoring by inverse histogram shifting.

4 EXPERIMANTAL RESULTS

We evaluated the proposed algorithm using 8 images which are 512x512 8 bits color images in USC-SIPI image database (see Fig. 6).

First, the image quality between an original JPEG compressed image and its watermarked JPEG compressed image is compared and summarized in Table 1. The PSNR value is calculated against a non-compressed original image.

Table 1: PSNR comparison (unit: dB).

Images	JPEG	w.JPEG	Difference
Airplane	37.68	34.33	3.35
Baboon	31.64	30.31	1.33
House	35.66	32.95	2.71
Lena	36.34	33.75	2.59
Peppers	35.16	33.02	2.14
Sailboat	33.55	31.82	1.73
Splash	38.42	35.18	3.24
Tiffany	36.13	33.68	2.45
Average	35.57	33.13	2.44

Although the watermarked JPEG images showed tiny noisy pattern on flat area, there were not easily recognizable. Also, note that the original quality can be restored in our algorithm. The PSNR degradation is 2.44dB on average and it supports that the watermark insertion does not degrade the image quality.

Figure 6: 8 Test images for experiments.

Table 2: Compression ratio comparison (Unit: %).

Images	JPEG	w.JPEG	Difference
Airplane	93.77	92.27	1.50
Baboon	86.69	84.79	1.90
House	91.84	90.26	1.58
Lena	93.77	92.11	1.66
Peppers	92.90	91.80	1.10
Sailboat	91.07	89.37	1.70
Splash	94.59	93.19	1.40
Tiffany	93.55	92.00	1.55
Average	92.27	90.65	1.62

We compared image compression ratio between an original JPEG compressed image and its watermarked JPEG compressed image (refer Table 2). The compression ratio of the original JPEG and the watermarked JPEG was 92.27% and 90.65% on average, respectively. The difference of each compression ratio is 1.63% which is small enough.

5 CONCLUSIONS

This paper presented a JPEG authentication algorithm using reversible watermarking, which can authenticate the integrity of JPEG compressed images because it is sensitive against attacks. Also, it has no large difference with an original JPEG compressed image in aspect of the image quality and the compression ratio. The proposed algorithm considers the re-saving or re-compression without any modification as a kind of attacks because it modifies the quantization DCT coefficients. Some applications require robustness against these processing. Future works is studying the algorithm to support this requirement.

ACKNOWLEDGEMENTS

This research project was supported by Ministry of Culture, Sports and Tourism (MCST) and from Korea Copyright Commission in 2011 and Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2011-0005129).

REFERENCES

Yuan, H., Zhang, X.-P., 2003, Fragile watermark based on the Gaussian mixture model in the wavelet domain for image authentication, *Proc. of Int. Conf. on Image Processing*, vol. 1, pp. I-505-8.

Hu, Y.-P., Han, D.-Z., 2005, Using two semi-fragile watermark for image authentication, *Proc. of Int. Conf. on Machine Learning and Cybernetics*, pp. 5484-5489.

Wang, H., Liao, C, 2009, Compressed-domain fragile watermarking scheme for distinguishing tampers on image content or watermark, *Proc. of Int. Conf. on Communications, Circuits and Systems*, pp. 480-484.

C. T. Li, 2004. *Vision, Image and Signal Processing, IEE Proceedings*, 2004, "Digital fragile watermarking scheme for authentication of JPEG images".