COMPRESSION AND PROTECTION OF JPEG IMAGES

Yi-Chong Zeng[1], Fay Huang[2], and Hong-Yuan Mark Liao[3]

[1,3]Institute of Information Science, Academia Sinica, Taiwan
[2,3]Institute of Computer Science and Information Engineering, National Ilan University, Taiwan
[1]yichongzeng@iis.sinica.edu.tw, [2]fay@niu.edu.tw, [3]liao@iis.sinica.edu.tw
+886-2-27883799 ext. 2419

ABSTRACT

The objective of this research is to design a new JPEG-based compression scheme which simultaneously considers the security issue. Our method starts from dividing image into non-overlapping blocks with size 8×8. Among these blocks, some are used as reference blocks and the rest are used as query blocks. A query block is the combination of the residual and the resultant of a filtered reference block. We put our emphasis on how to estimate an appropriate filter and then use it as part of a secret key. With both reference blocks and the residuals of query blocks, one is able to encode secured images using a correct secret key. The experiment results will demonstrate that how different secret keys can control the quality of restored image based on the priority of authority.

Index Terms – Joint Photographic Experts Group (JPEG), image compression, content protection

1. INTRODUCTION

Everyday a huge number of images are delivered through the Internet. People start to realize the importance of image authorization and content protection. Among the huge number of image delivered daily, most of them are encoded by JPEG standard. JPEG standard is now in common use over all lossy compression technology of still image [1, 2]. Although JPEG-2000 has many advantages over JPEG [3], for example: less visible artifact, no blocky effect, rand code-stream access and processing, high compression rate, etc, up to now, people still like to use JPEG rather than JPEG-2000 to compress still images.

For a baseline JPEG standard, it is composed of several phases, including colorspace transform, offsetting, discrete cosine transform (DCT), quantization, differential pulse-code modulation (DPCM), run-length encoding (RLE), and variable-length coding (VLC). To securely protect targeted images, the best strategy is to manipulate the data in JPEG domain. That is, at the phases of DCT coefficients, run-length encoding, and variable-length coding.

Conventionally, researchers modify DCT coefficients to implement watermarking, data hiding, and encryption in multimedia. Most of the existing DCT-based watermarking approaches were developed to authenticate JPEG-based images or MPEG-based videos. In [4, 5], Hsu and Wu proposed DCT-based watermarking for image and video. They proposed to modify 16 middle-frequency DCT coefficients so that the hidden watermark is imperceptible. Similar watermarking approaches have been addressed in [6], the watermark bits are embedded into four DCT coefficients which include one DC value and three low-frequency AC values. The characteristics of the previous work is that the watermark can be extracted from a covered image in spatial domain and DCT coefficients in transform domain.

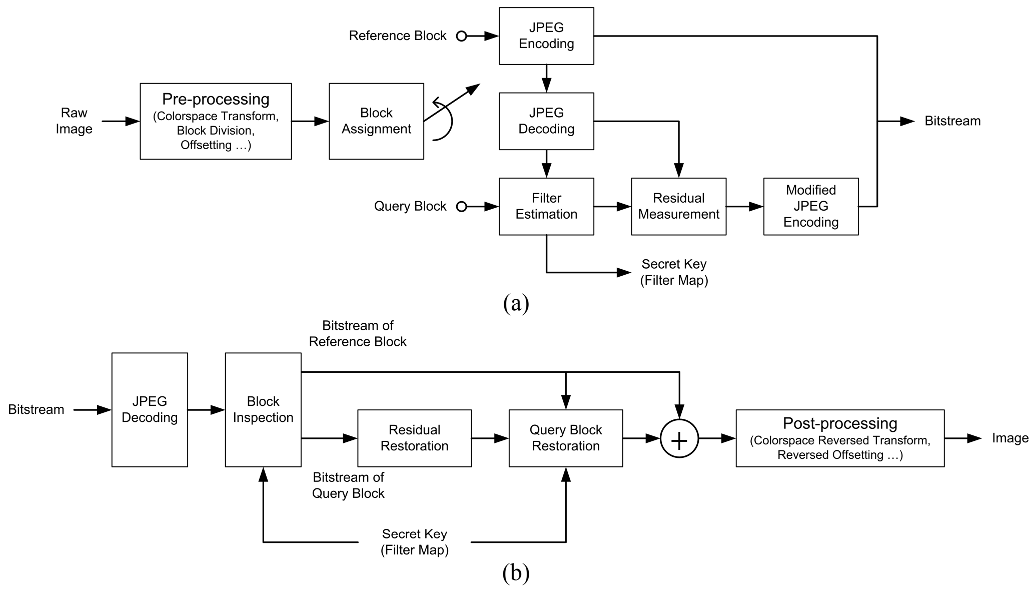
To better secure the encryption of multimedia, some researchers made use of multiple Huffman table (MHT) to encrypt data rather than working on DCT coefficients directly. In [7], Wu and Kuo proposed an MHT-based encryption scheme. They applied their approach on JPEG images as well as MPEG videos. In [8], Xie and Kuo presented an enhanced MHT scheme to resist the chosen plaintext attack. In addition to the work that put emphasis on encrypting multimedia data, some researchers were interested in considering both the compression and the security issues simultaneously. In [9], Wu and Kuo proposed ways to integrate both encryption and compression simultaneously. They analyzed different encryption schemes and then decided whether a chosen scheme can be combined with a compression scheme. They employed multiple statistical models to convert Huffman codes into encryption ciphers. In [10], Zhou also addressed the issue of joint compression and watermarking on JPEG images.

The objective of this research is to design a new JPEG-based compression scheme which is able to satisfy the requirement of security at the same time. In the first step, we divide an image into non-overlapping 8×8 blocks. Among these blocks, some are used as reference blocks and the rest are used as query blocks. A query block is the combination of the residual and the resultant of a filtered reference block. Our research will be focused on how to estimate an appropriate filter and then use it as part of a secret key. With both reference blocks and the residuals of query blocks, one is able to encode secured images via JPEG standard. The rest of this paper is organized as follows. The proposed scheme will be described in Section 2. The way to protect the content of an image using different secret keys will be introduced in Section 3. Experiment results will be reported in Section 4, and the concluding remarks will be drawn in Section 5.

2. THE PROPOSED METHOD

In this work, we propose a new scheme to perform compression and content protection simultaneously. The major contribution of this scheme is that it does not need to either modify the DCT coefficients or alter the procedure of entropy coding. Our method is very different from the existing methods [4-10]. The block diagrams of the encoder and the decoder are shown in Figs.1(a) and 1(b), respectively. The details about how encoder and decoder operate will be introduced in the following sections.

978-1-4577-1302-6/11/$26.00 ©2011 IEEE



(a)

(b)

Fig.1. The block diagrams of (a) the encoder and (b) the decoder of the proposed method.

2.1. Encoder

The encoder of the proposed scheme consists of four steps, including: pre-processing, block assignment, filter estimation, and encoding.

2.1.1. Pre-processing

In the pre-processing step we implement the same work as in JPEG encoder. The R-G-B colorspace of an image is transformed into Y-C_b-C_r colorspace, and then the luminance component (Y) is subtracted with an offset of value 128. Then, the luminance component and two chrominance components are divided into non-overlapped blocks of size 8×8.

2.1.2. Block Assignment

The proposed method needs to classify all blocks into reference block and query block in advance. While some reference blocks are chosen, and the rest of blocks are query blocks. Every query block corresponds to only one reference block that is the nearest one. Fig.2 shows the arrangement of reference block.

2.1.3. Filter Estimation

One basic assumption of this work is that a query block should be similar to its nearest reference block. The relation between a query block and a reference block can be expressed as follows:

$$\mathrm{B_q} = \mathrm{B_r} \otimes \mathrm{F} + \mathrm{R}\,, \tag{1}$$

where $\mathrm{B_q}$ and $\mathrm{B_r}$ are, respectively, a query block and a reference block. The symbol '⊗' denotes the convolution operation. F and R represent, respectively, the filter and the residual of a query block. The filter F of size W_F×H_F is defined as,

$$\mathrm{F} = \begin{bmatrix} f(0,0) & f(1,0) & \cdots & f(W_\mathrm{F}-1,0) \\ f(0,1) & f(1,1) & & f(W_\mathrm{F}-1,1) \\ \vdots & \vdots & \ddots & \vdots \\ f(0,H_\mathrm{F}-1) & f(1,H_\mathrm{F}-1) & \cdots & f(W_\mathrm{F}-1,H_\mathrm{F}-1) \end{bmatrix}, \tag{2}$$

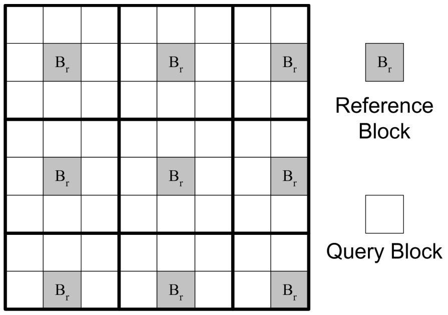


Fig.2. The arrangement of reference block

where $f(i,j)$ denotes the (i,j)-th coefficient of the filter, and $3 \leq W_\mathrm{F}$, $H_\mathrm{F} \leq 8$. In (1), the resultant after filtering a reference block is called a filtered block (which is abbreviated as $\mathrm{B_f}$) and it is expressed as follows:

$$\mathrm{B_f}(x,y) = \sum_{u=-\left\lfloor \frac{W_\mathrm{F}}{2} \right\rfloor}^{\left\lfloor \frac{W_\mathrm{F}-1}{2} \right\rfloor} \sum_{v=-\left\lfloor \frac{H_\mathrm{F}}{2} \right\rfloor}^{\left\lfloor \frac{H_\mathrm{F}-1}{2} \right\rfloor} \mathrm{B_r}(x+u,y+v)\cdot f(u+\left\lfloor \tfrac{W_\mathrm{F}}{2} \right\rfloor, v+\left\lfloor \tfrac{H_\mathrm{F}}{2} \right\rfloor)\,, \tag{3}$$

The function of $\lfloor x \rfloor$ is a floor operation and it usually results in the largest integer which is equal to or smaller than x. To turn (3) into matrix form, it is formulated as follows:

$$\begin{bmatrix} \mathrm{B_f}(0,0) \\ \mathrm{B_f}(0,1) \\ \vdots \\ \mathrm{B_f}(7,7) \end{bmatrix} = \begin{bmatrix} 0 & \cdots & \mathrm{B_r}(0,0) & \mathrm{B_r}(1,0) & \cdots \\ \cdots & \mathrm{B_r}(0,0) & \mathrm{B_r}(1,0) & \mathrm{B_r}(2,0) & \cdots \\ \vdots & & \vdots & & \vdots \\ \cdots & \mathrm{B_r}(6,7) & \mathrm{B_r}(7,7) & \cdots & 0 \end{bmatrix} \begin{bmatrix} f(0,0) \\ f(0,1) \\ \vdots \\ f(W_\mathrm{F}-1,H_\mathrm{F}-1) \end{bmatrix}, \tag{4}$$
$$\Updownarrow$$
$$\mathrm{P_f} = \mathrm{P_r}\Phi$$

where $\mathrm{P_f}$ and Φ denote the column vectors of $\mathrm{B_f}$ and F, respectively. Let $\mathrm{P_q}$ be the column vector of $\mathrm{B_q}$. The least-square-estimation (LSE) can be used to estimate the filter in (4). $\mathrm{P_f}$ can be replaced by $\mathrm{P_q}$, and Φ can be computed according to,

$$\Phi = (\mathrm{P_q^T P_r})^{-1}\mathrm{P_q^T P_q}\,, \tag{5}$$

where $\mathrm{P^T}$ represents the transpose of the column vector P. Subsequently, the estimated filter is put into (4) to yield the filtered block, and the residual of the query block is computed by subtracting the filter block from the query block. Consequently, the estimated filters of all blocks can be constructed as a filter map (FM) and this map can be used as a secret key.

2.1.4. Encoding

Both of the reference blocks and residuals are encoded via JPEG compression standard. However, a slight modification is the calculation of the differential pulse-code modulation (DPCM). In conventional JPEG, the value obtained by DPCM is the difference of DC coefficients corresponding to two consecutive blocks. In the proposed method, we first calculate the DPCM value between two consecutive reference blocks. Subsequently, the DPCM value between two residuals of the consecutive query blocks is computed in the same group. The same quantization table and entropy code are adopted to operate on the reference blocks and residuals.

2.2. Decoder

In our scheme, the calculated filter map can be used to decode the compressed data. With this filter map, we are able to identify whether a block is a reference block and we can then restore the image. In the decoding process, if a block is identified as a query block, its corresponding residual is decoded; otherwise, its corresponding reference block is decoded. For a query block, if its corresponding filter and its nearest decoded reference block are available, then the query block can be restored based on (1). Subsequently, we perform reverse colorspace transform as well as reverse offsetting to completely decode the image.

3. CONTENT PROTECTION

As we mentioned in Section 2.2, a filter map can be thought of as a secret key. Without the map, we cannot distinguish from reference blocks and query blocks. Under these circumstances, an original image cannot be restored correctly. Therefore, a filter map can be used as a key to control the degree of image restoration. A typical application is to result in an image generation system that can generate images with different clarity based on the degree of authority of receivers. For a user with low authority, he/she can only decode low quality images. For a user with high authority, on the other hand, he/she can decode high quality images. To achieve this, we use existing blurring schemes (such as Gaussian filtering, 2D lowpass filtering) to degrade the quality of an original image. Then, we use the proposed method to operate on both the original image and the blurred image. Through this operation, we can obtain two filter maps, FM$_{\text{orignal}}$ and FM$_{\text{blurred}}$, respectively. The compressed data of the original image is transmitted to the user. However, the low-authority user will receive the secret key FM$_{\text{blurred}}$ to obtain a blurred image. The full-authority user can obtain the good-resolution image by receiving the secret key FM$_{\text{original}}$.

4. EXPERIMENT RESULTS

4.1. Image Restoration with/without Secret Key

In this experiment we would show how a secret key influences the image restoration results. For this experiment, a 95% quality factor and 3×3 filter for every query block were chosen. On the other hand, we adopted the arrangement of reference block as shown in Fig.2. A test image with size 240×240 is shown in Fig.3(a). Fig.3(b) shows the combination of reference blocks and corresponding residuals. It is obvious that if a secret key was not used, only reference blocks and the corresponding residuals were decoded in this case. The content shown in Fig.3(b) is fragile and dim. By using the correct filter map (secret key), a much better filtered image were restored as indicated in Fig.3(c). Adding Fig.3(b) and Fig.3(c) together, we were able to restore a complete image with high peak signal-to-noise ratio (PSNR) as shown in Fig.3(d) with 43.47dB. To replace the original filter with a two-dimensional delta function, Fig.3(e) shows the filtered image.

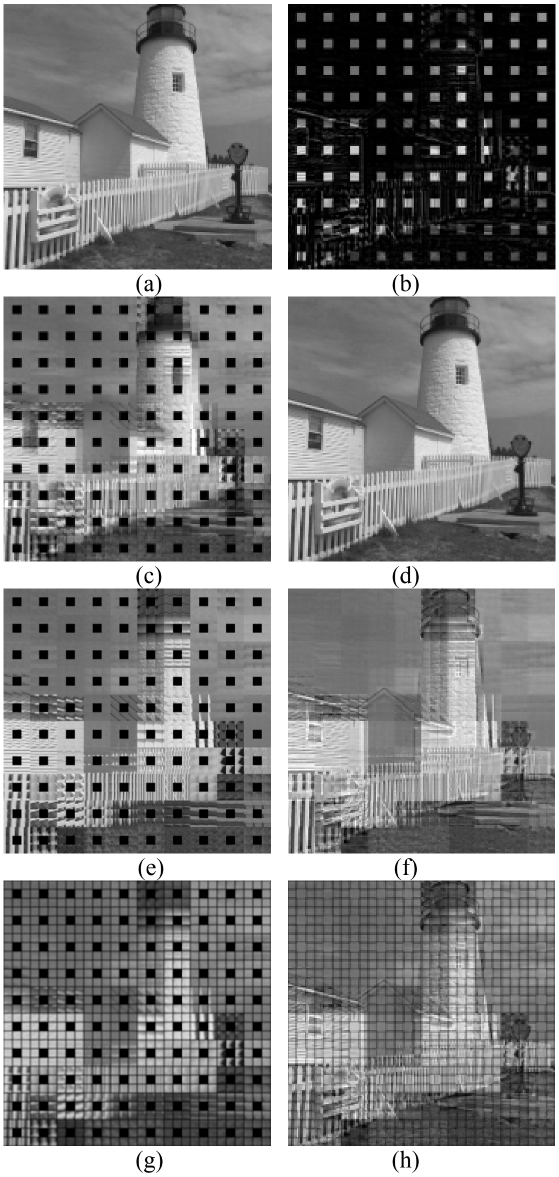


Fig.3. Image Restoration: (a) original image; (b) combination of reference blocks and residuals (PSNR=6.00dB); (c) filtered image using the correct secret key; (d) the restored image of (b)+(c) (PSNR=43.47dB); (e) filtered image using 2D delta function; (f) the restored image of (b)+(e) (PSNR=18.62dB); (g) filtered image using average filter; and (h) the restored image of (b)+(g) (PSNR=16.19dB).

Under these circumstances, the restored image can be synthesized by adding Figs.3(b) and 3(e) together and shown in Fig.3(f). It is apparent that the quality of the restored image was bad (PSNR=18.62dB). Fig.3(g) shows the filtered image using average filter and the final restored image (which is combination of Figs.3(b) and 3(g)) is shown in Fig.3(h). Again, it is apparent that if a wrong secret key (filter map) was used, the quality of a restored image could be as low as 16.19dB.

4.2. Content Protection

In this section we shall report how a content protection mechanism can be realized by the proposed method. Based on the filter map estimation procedure described in Section 3, the filter maps of an original image as well as its blurred version can be estimated. Under these circumstances, only the compressed version of an original image has to be transmitted to a user. For a user who has only low authority, he/she only retains the low-authority key, $FM_{blurred}$, to restore a poor-resolution image. On the other hand, a user who has high authority, he/she can use the high-authority key, $FM_{original}$, to restore a high-resolution image. The restored poor-resolution image (PSNR=20.15dB) and high-resolution image (PSNR=39.70dB) are shown in Figs.4(a) and 4(b), respectively.

4.3. Compression Performance against Filters with Various Sizes

In the third experiment we conducted experiments to analyze how the size of a filter map influenced the quality of restored images. The image shown in Fig.3(a) was adopted to conduct experiments. We chose four different filter sizes, including 3×3, 5×5, 7×7, and 8×8 filters to test on Fig.3(a). In addition, we also adjusted the quantization table so that the encoded data at various quality levels could be computed. Fig.5 shows five curves which correspond to the results generated by four different filter sizes and conventional JPEG. From Fig.5, it is obvious that a small-sized filter needs more bits to encode an image under the constraint of the same quality. Fig.5 also indicates that a large-sized filter could achieve better compression results than JPEG. From Fig.5, it is amazing that if one adopts the 8×8 filter, he/she only needs less than 1 bit-per-pixel to encode an image with high quality.

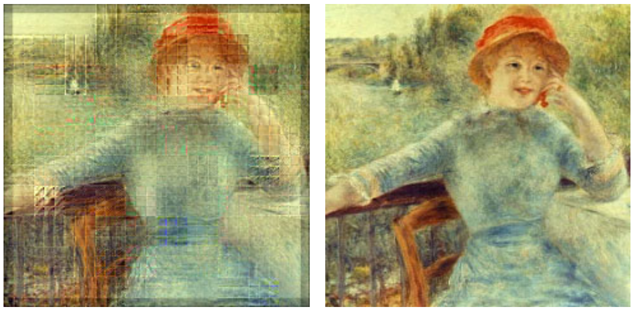

(a) (b)

Fig.4. Content Protection: (a) The restored image using low-authority key (PSNR=20.15dB), (b) restored image using high-authority key (PSNR=39.70dB)

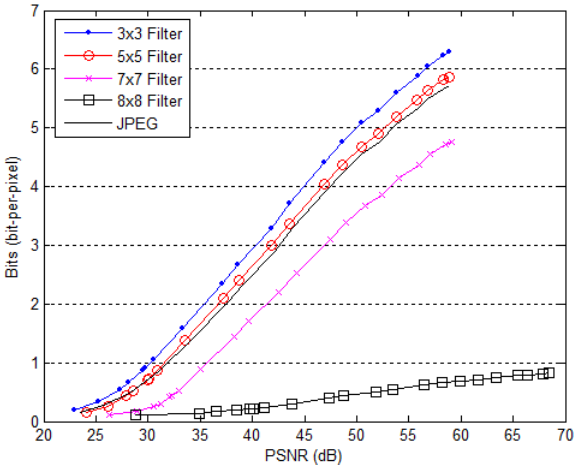


Fig.5. Compression Performance: The proposed method was applied to Fig.3(a) with four different filter sizes. We adjusted the quantization table in order to compute the size of encoded data under various quality levels.

5. CONCLUSION

We have proposed a new JPEG-based compression scheme which considers the security issue simultaneously. We divided an image into non-overlapping blocks with size 8×8, and used some of them as reference blocks and the rest as query blocks. We developed a systematic way to estimate an appropriate filter and then used it as part of a secret key. Once a person has both reference blocks and the residuals of query blocks, he/she is able to encode secured image using a correct secret key.

REFERENCES

[1] W. B. Pennebaker and J. L. Mitehell, JPEG: Still Image Data Compression Standard, Van Nostrand Reinhold, New York, 1992.

[2] http://en.wikipedia.org/wiki/JPEG#The_JPEG_standard

[3] http://en.wikipedia.org/wiki/JPEG_2000

[4] C.-T. Hsu and J.-L. Wu, "DCT-Based watermarking for video," *IEEE Trans. Consumer Electronics*, vol. 44, no. 1, pp.206-216, Feb. 1998.

[5] C.-T. Hsu and J.-L. Wu, “Hidden digital watermarks in images," *IEEE Trans. Image Processing*, vol. 8, no. 1, pp.58-68, Jan. 1999.

[6] Y.-C. Zeng, S.-C. Pei and J.-J. Ding, “DCT-based image protection using dual-domain bi-watermarking algorithm,” *ICIP*, Atlanta, GA, USA, pp.2581-2584, Oct. 2006.

[7] C.-P. Wu and C.-C. Jay Kuo, "Efficient multimedia encryption via entropy codec design," *in Proc. of SPIE vol.4314, Security and Watermarking of Multimedia Contents III*, pp.128-138, Jan. 2001

[8] D. Xie and C.-C. Jay Kuo, “Enhanced multiple Huffman table (MHT) encryption scheme using key hopping,” *ISCAS*, vol.5, pp.568-571, May 2004.

[9] C.-P. Wu and C.-C. Jay Kuo, "Design of integrated multimedia compression and encryption systems," *IEEE Trans. Multimedia*, vol.7, no.5, pp.828-839, Oct. 2005.

[10] Y. Zhou, “Joint compression and watermarking using variable-rate quantization and its applications to JPEG,” Master Thesis, University of Waterloo, 2008. http://uwspace.uwaterloo.ca/bitstream/10012/4260/1/Yuhan %20Zhou-MASc-thesis.pdf