Semi-fragile Watermarking Technique for a Digital Camera

Myung-Eun Lee, Hyun Lim, Soon-Young Park, Seong-Jun Kang, Wan-Hyun Cho*

School of Information Engineering, Mokpo National University

Dept. of Statistics, Chonnam National University*

E-mail : melee@mokpo.ac.kr

Abstract

In this paper, we present a digital image authentication using semi-fragile watermarking techniques. The algorithm is robust to innocuous manipulations while detecting malicious manipulations. Specifically, the proposed method is designed for the purpose of the real time authentication of an image frame captured from a digital camera due to its easy H/W implementation, security and visible verification.

To achieve the semi-fragile characteristics that survive a certain amount of compression, we employ the invariant property of DCT coefficients' quantization proposed by Lin and Chang [1]. The binary watermark bits are generated by exclusive ORing the binary logo with pseudo random binary sequences. Then watermark bits are embedded into the LSBs of pre-quantized DCT coefficients in the medium frequency range. Verification is carried out easily due to visually recognizable pattern of the logo extracted by exclusive ORing the LSBs of the embedded DCT coefficient with pseudo random number seeded by a secret key.

By the experiment results, this method is not only robust to JPEG compression but also it detects powerfully alterations of the original image, such as the tempering of images.

I. Introduction

The goal of authentication is to verify that the original contents have not been modified up to a particular level. Different types of digital watermarks have recently been proposed as the means to authenticate the content of the digital multimedia [2]. Watermarking techniques for image authentication are usually designed to be fragile or semi-fragile watermarks according to their robustness, and can be grouped into spatial domain method or transform domain method according to their embedding approaches.

The fragile method has evolved first under the assumption that any manipulations modify the embedded watermark. Yeung et al. use a pseudo random sequence seeded by a key-dependent function to embed a binary watermark to an image, so that any modifications to the image can be detected [3]. Wong et al. propose a watermark that allows a user with an appropriate key to verify the integrity and ownership of an image [4]. In this method, the LSBs of a block-based image is replaced by the exclusive OR operation results between the hash output and the block of a binary watermark. The fragile watermarking techniques are generally processed on the spatial domain.

Recently, image authentication by means of semi-fragile watermarking becomes increasingly popular in the sense that it can distinguish between malicious and innocuous manipulations unlike the fragile watermarking techniques. To achieve the semi-fragile characteristics that survive a certain amount of compression, most of the proposed semi-fragile watermarking approaches perform embedding in the transform domain.

The invariant property of DCT coefficients' quantization has been employed by Lin and Chang to develop the semi-fragile watermarking technique accepting JPEG lossy compression [1]. This method can embed authentication bits and recovery bits into the pre-quantized DCT coefficients being capable of identifying the position of altered blocks and recovering them approximately. To improve the Lin and Chang's method, Maeno et al. have proposed other semi-fragile authentication technique using random bias and nonuniform quantization and extended the DCT domain-based method to the wavelet domain [5].

Most watermarking algorithms have been developed for software implementations due to ease of use, upgrading and flexibility. However, the software implementations have the limited speed problem and are vulnerable to the off-line attacks. Therefore it may be desirable to watermark the image inside the digital image acquisition device such as a digital camera to authenticate the original data content, since the off-line watermarking process cannot guarantee the tamper-proof.

In this paper, we present a semi-fragile watermarking technique that is the modification of Lin and Chang's method based on the invariant property of quantization. To employ the

proposed algorithm for the real time authentication of an image frame captured from a digital camera, this method focuses on robustness to JPEG compression, easy implementation, security and visible verification.

II. Digital Camera Scheme

A digital camera is a portable device to capture an image frame from scene and store it on the flash memory. Here we consider adding a watermark embedding operation to the conventional digital camera to authenticate every captured image before storing it on its nonvolatile memory. The architecture of a digital camera scheme is shown in Fig. 1.

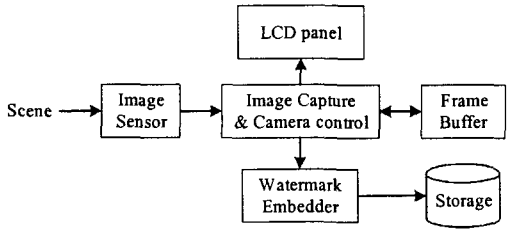

Fig. 1. The block diagram of a digital camera added with watermarking technique.

In order to capture natural scene images, the scheme have *acquired an image frame from the image sensor.* The captured image is temporarily stored in an internal medium, consisting of the frame buffer. Then the image frames are continuously displayed on the LCD to control the LCD panel. The watermark embedder inserts authentication bits to the selected image frame and send it to storage. In the section III, we introduce an efficiency algorithm for a digital camera.

III. Image Authentication Algorithm

The block diagram of the proposed image authentication algorithm is given in Fig. 2. In order to insert the watermark, we first partition an image into blocks of size 8×8 and apply DCT to each block. Let $\{C(i,j), 0 \le i,j \le 7\}$ be the DCT coefficients for arbitrary block. After quantizing the coefficients with predefined quantization array $Q(i,j)$ we have the following relation.

$$\hat{c}(i,j) = round[\frac{C(i,j)}{Q(i,j)}] \quad (1)$$

where $round$ is a function to denote the nearest integer operation. Applying dequantization to $\hat{c}(i,j)$ yields the dequantized vector $\hat{C}(i,j)$ which is the integral multiple of quantization matrix $Q(i,j)$.

$$\hat{C}(i,j) = \hat{c}(i,j)Q(i,j) \quad (2)$$

Lin and Chang have proved that the vector $\{\hat{C}(i,j)\}$ can be reconstructed after allowable JPEG lossy compression if the subsequent quantization step used in JPEG compression is smaller than $\{Q(i,j)\}$ [1]. In this paper, we also use the invariant property of quantized vector $\{\hat{c}(i,j)\}$ to develop the semi-fragile watermarking technique. The original coefficients are first replaced by $\{\hat{C}(i,j)\}$ to use the invariant property of quantized vector at the expense of distortion due to pre-quantization of $\{Q(i,j)\}$ and then watermark embedding and extraction process are followed from $\{\hat{c}(i,j)\}$.

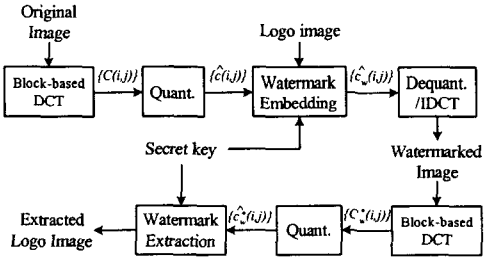

Fig. 2. The block diagram of a proposed image authentication algorithm.

3.1 Procedure of watermark embedding

Block diagram for inserting authentication watermarks to each block is shown in Fig. 3. Let $\{c_{00}, c_{01}, c_{10}, \cdots, c_{77}\}$

denote the elements of quantized vector $\{\hat{c}(i,j)\}$ computed from an arbitrary block. Here c_{00} at the origin is the DC component representing the brightness in the image and other elements belong to AC components related to the gray level changes in the image. To avoid the Holliman-Memon attack by using the same authentication bits for each block we concatenate the block number with a secret key hard-wired in the camera to select the seed number [6]. The binary pseudo random numbers are generated with the seed number and exclusive ORed with a chosen binary logo as follows.

$$w_i = a_{mn} \oplus p_i \tag{3}$$

where a_{mn} is the elements in the binary logo, p_i is the binary random number and $\oplus$ is the exclusive OR operation. Then w_i is inserted into the LSBs of $\{\hat{c}(i,j)\}$ in the medium frequency range. The embedded coefficients $\{\hat{c}_w(i,j)\}$ are dequantized using $\{Q(i,j)\}$ and inverse discrete cosine transformed to yield the watermark embedded image.

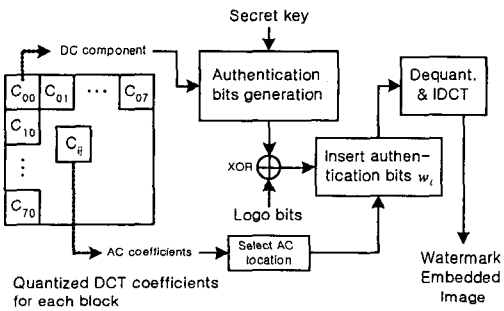

Fig. 3. Block diagram showing the procedure for inserting an authentication watermarks to each block.

3.2 Procedure of watermark extraction

To extract the authentication bits from the watermark embedded image, 8×8 block based DCT transform is applied to each block and pre-quantized vector is computed in a similar manner as embedding process. Then exclusive ORing the LSBs of the quantized coefficients with pseudo random number seeded by a secret key yields the authentic logo bits as shown in Fig. 4.

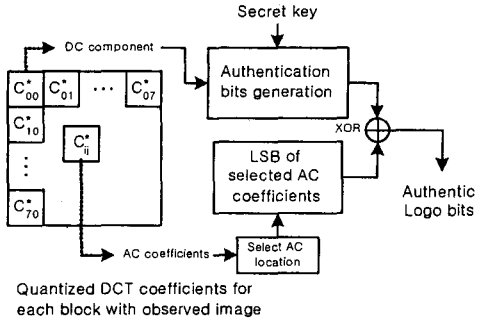

Fig. 4. Block diagram of the extraction procedure

IV. Experimental results

To test our proposed algorithm, we use the 480×640 gray-level "tulips" image as shown in Fig. 5. Our logo image is constructed by 120×160 binary pattern as shown in Fig. 6. After pre-quantizing the block-based DCT transformed original image with quantization step $Q(i,j) = Q_C(i,j)+1$, where $Q_C(i,j)$ is the quantization step being used in later JPEG compression, we embed 4 authentication bits into the quantized coefficient vector. Fig. 7 shows the JPEG compressed image with quality factor 75 after watermark embedding. As we can see, the watermarked image looks similar to the original one without any visible artifacts. The results of watermark extraction from the embedded image of Fig. 7 are shown in Fig. 8. The watermarked image can survive JPEG compression using the proper secret key, but the random noise pattern is returned with an incorrect key.

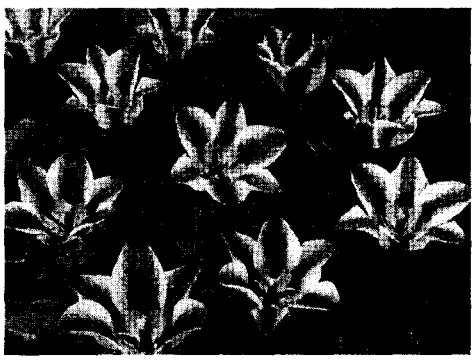

Fig. 5. Test image.

Fig. 6. Logo image.

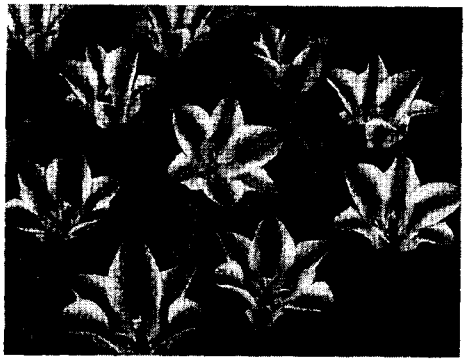

Fig. 7. JPEG compressed image after watermark embedding.

(a) (b)

Fig. 8. Extracted logo image (a) use of a correct key, (b) use of an incorrect key.

Fig. 9 shows an altered version of the original image obtained after inserting other flower petal and text. We can see that the extracted logo image of Fig. 10 can identify the manipulated locations. Using visually recognizable logo pattern we can authenticate the test image easily.

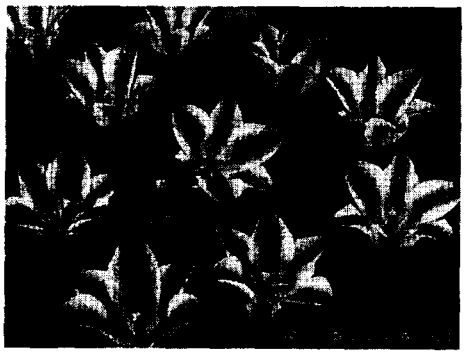

Fig. 9. Watermarked image after modification.

Fig. 10. Extracted logo image from modified image.

V. Conclusions

We present a semi-fragile watermarking technique for a digital image authentication. We employ the invariant property of DCT coefficients' quantization to achieve the semi-fragile characteristics that survive a certain amount of JPEG compression. The binary watermark bits are generated by exclusive ORing the binary logo with pseudo random binary sequences. To avoid the Hollima-Memon attack by using the same binary logo and the same secret key, pseudo random numbers are generated by using the block dependent seed number. Watermark bits are embedded into the LSBs of pre-quantized DCT coefficients in the medium frequency range. Verification is carried out easily due to visually recognizable pattern of the logo extracted by exclusive ORing the LSBs of the embedded DCT coefficient with pseudo random number. From experimental results, we note that the proposed technique is robust to JPEG compression and detects efficiently the malicious manipulations.

References

[1] C.-Y. Lin and S.-F. Chang, "Semi-Fragile Watermarking for Authenticating JPEG Visual Content," *SPIE Security and Watermarking of Multimedia Contents II, EI'00,* San Jose, CA, Jan. 2000.

[2] Bibliography of Multimedia Authentication Research Papers, http://www.ctr.columbia.edu/~cylin/auth/bibauth.html, 2003.

[3] F. Minzer, G. W. Braudaway, and M. M. Yeung, "Effective and Ineffective Digital Watermarks," *IEEE International Conference on Image Proceedings, Vol. 3,* pp 9-12, Santa Barbara, USA, 1997.

[4] P. W. Wong and N. Memon, "Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification," *IEEE Trans. on Image Processing, Vol.10, No.10,* Oct. 2001.

[5] K. Maeno, Q. Sun ,S. Chang and M. Suto, "New Semi-Fragile Image Authentication watermarking Techniques Using Random Bias and Non-Uniform Quantization," *EI2002,* San Jose, USA, Jan. 2002.

[6] J. Fridrich, "Security of Fragile Authentication Watermarks with Localization," *Proc. of SPIE Photonic West, Vol.4675, I 2002, Security and Watermarking of Multimedia Contents,* San Jose, USA, Jan. 2002.