A DCT-based Recoverable Image Authentication Technique

Hsien-Chu Wu[1], Chin-Chen Chang[2] and Ting-Wei Yu[1]

[1]Department of Information Management
National Taichung Institute of Technology, Taichung City, Taiwan, 404, R.O.C.
[2] Department of Information Engineering and Computer Science,
Feng Chia University, Taichung, Taiwan, 40724, R.O.C.

Abstract

In this paper, a scheme that has tamper proofing and recovery abilities is proposed. With the specific DCT frequency coefficients taken as the characteristic values, which are embedded into the least significant bits of the image pixels, it is used to provide proof of image integrity. If the image is tampered, the embedded characteristic values that are affected will be changed accordingly and then detected. Then the corresponding original characteristic values can be acquired by the proposed recovery process to reconstruct the image.

Keywords: DCT, tamper detection, tamper proofing

1. Introduction

Because of the Internet, people are provided with many types of convenient services and an unending flow of information. This is significant, especially with relation to data processing that utilizes digitalized media such as audio, images, video, etc. Of all digital media applications, digital imagery is the most popular but it can be easily distributed, copied, and tampered. Because of this, protecting the integrity of the intellectual property of images by recognizing when it has been tampered is a pressing research matter.

In recent years, much related tamper proofing research [1, 2, 4, 7-11] has been published. Walton [8] first proposed the image tamper detection technique. For an original gray-level image, this method calculates the checksums of the seven most significant bits (MSBs) of the image and embeds them into the significant bits of the randomly chosen pixels. Walton's technique is very effective for tamper detection. However, it is possible to modify the lowest significant bits (LSBs) which contain the verification information. Furthermore, it does not possess recoverability ability. Yang, Huang and Tang's technique [11] focused on tampered positions in the image. This method utilizes the RSA encryption procedure [5, 6] to encrypt the blocks made up of the MSBs that have been processed through hashing functions so that the digital signature is yielded. The acquired digital signature is then placed into the LSBs of the original image as a reference to the proof of the integrity of the image. This method doesn't posses the ability to restore the image. Lin and Fu's image authentication method [4] is based on using the invariance of the relationship between Discrete Cosine Transformation (DCT) [3] coefficients at the same position in separate blocks of an image to generate feature codes for each protected image. After encryption is applied to the feature codes, the signature is produced and kept secret by the authorized users to verify whether or not the received image has been tampered with. However, it cannot restore the image. All of the published image proof techniques place great emphasis on proof of tampered position without possessing the ability to restore the tampered image. These techniques obviously need to be improved upon to restore the image.

In this paper, the proposed scheme introduces a brand-new proof that points out the tampered positions in the image and restores the image. The proposed scheme applies DCT to take certain frequency coefficients from the image as the characteristic values for the image and encrypts the characteristic values. Next, it randomly embeds those encrypted characteristic values into the LSBs of the randomly assigned pixels of the original image. Finally, a public stego-image is produced. Whenever the stego-image needs to be verified for tamper tracing, the proposed tamper detection process first gets the embedded characteristic values from the stego-image and the values calculated from the stego-image and then compares them with each other. Each unmatched area is a sign that the stego-image is tampered. Then, the proposed recovery process restores the image using the characteristic values of the original image.

2. The Proposed Scheme

In order to protect the intellectual property of the digital image, the proposed scheme primarily acquires characteristic values of the original image for tamper proofing and applies embedded characteristic values of the image to restore the image so as to authenticate its copyright.

2.1. Embedding Process

Let the protected original image be gray-level image O of $N\times N$ pixels. Image O is defined in Equation (4) as

$$O=\{o(i,j)|\ 0\leqq o(i,j)\leqq 255,\ 0\leqq i,j\leqq N\text{-}1\ \}. \tag{4}$$

Since the characteristic values of the original image O will be hidden into two LSBs of each image pixel, the initial procedure is to set the last two LSBs in each pixel $o(i,j)$ to be zero. Let the modified image be O_t.

To boost the trial operation of DCT, the divided block of the image that will be converted has to be kept small. First, O_t is divided into non-overlapped blocks BS_i's, such that each block BS_i contains $M\times M$ pixels, i= 0,1, …, $(N/M)\times(N/M)$-1. Then DCT is applied to each individual BS_i. Let BF_i=DCT(BS_i) and $M\times M$ frequency coefficients in BF_i in zigzag order be $DC^i, AC_0^i, AC_1^i, ..., AC_{(M\times M)-2}^i$.

Each block BS_i provides the maximum storage for the embedded characteristic values of $M\times M\times 2$ bits and, if it is expanded into the entire original image, there will be a maximum number of $N\times N\times 2$ bits. If a frequency coefficient takes up k bits, the maximum number of extracted characteristic values in each BF_i is $N\times N\times 2/k$, denoted to be X. Let Y be a predefined parameter to represent the extracted number of characteristic values from each BF_i and $0<Y\leqq X$. In the acquisition procedure, the Y frequency coefficients $DC^i, AC_0^i, AC_1^i, ..., AC_{Y-2}^i$ construct a set CV_i and it is taken for the characteristic of each BS_i.

To enhance the accurancy, there is verification data inserted into each characteristic value in CV_i before it is embedded. Let the binary form of each characteristic value in CV_i be expressed as ($B_{a,k-1}^i, B_{a,k-2}^i$, …, $B_{a,0}^i$), a=0, 1, …,Y -1. A secret key K_1 is assigned as the seed of PRNG. PRNG(K_1) is then performed to build a random bit stream P^i of $Y\times(k\text{-}2)$ bits. Non-overlappingly, with every (k-2) bits as a unit, break P^i into sub-streams P_a^i's. The binary form of P_a^i can be simply expressed as ($BP_{a,k-3}^i$, $BP_{a,k-4}^i$,…, $BP_{a,0}^i$). After retrieving the first (k-2) bits from each characteristic value to make CP_a^i, represented by $B_{a,k-1}^i, B_{a,k-2}^i$, …, $B_{a,2}^i$, each P_a^i as well as each CP_a^i will be sequentially calculated according to Equation (5). Using the calculation in Equation (5), the resulting value r_a^i representing the verification data is used to alter the last two LSBs, $B_{a,1}^i$ and $B_{a,0}^i$, of the corresponding characteristic value. When each of the verification data is inserted into the characteristic value, let the modified CV_i be CV_i'.

$$B_{a,1}^i, B_{a,0}^i = \begin{cases} 0,0 & \text{if } r_a^i = 0 \\ 0,1 & \text{if } r_a^i = 1 \\ 1,0 & \text{if } r_a^i = 2 \\ 1,1 & \text{if } r_a^i = 3 \end{cases} \tag{5}$$

, where $r_a^i = \left(\sum_{m=2}^{k-1}\left(B_{a,m}^i \text{ OR } BP_{a,m-2}^i\right)\right) \bmod 4.$

The characteristic values are copied as H sets. Here, $H = \lceil X/Y \rceil$. So far each BS_i has one set of CV_i', and that set of CV_i' has to be copied as H sets to generate CV_i'', but the value of H depends upon X and Y. When X/Y is an interger, the last set of characteristic values of CV_i''will duplicate all Y frequency coefficients from CV_i'. In contrast, the last set of characteristic values of CV_i'' will only contain the first y frequency coefficients, where $y = X\text{-}(H\text{-}1)\times Y$.

An extra encrypting procedure is needed to enhance the security. Our scheme for encrypting CV_i'' first assigns another secret key K_2 as the seed of PRNG to build a binary random sequence G^i with $X\times k$ bits. Non-overlappingly, with every k bits as a unit, partition G^i into subsequence G_b^i, b=0, 1, …, X-1, where each G_b^i is expressed in a binary unit as $BG_{b,m}^i$, m=0, 1, …, k-1. On the other hand, express each coefficient of CV_i'' in a binary format to make $CB_{b,m}^i$. Now, according to Equation (6), logical exclusive-OR operation XOR is sequentially executed on each $BG_{b,m}^i$ and $CB_{b,m}^i$ to generate encrypted $BW_{b,m}^i$. After all coefficients in CV_i'' have been encrypted, let all $BW_{b,m}^i$'s be represented by E_i.

$$BW_{b,m}^i = CB_{b,m}^i \text{ XOR } BG_{b,m}^i. \tag{6}$$

To enhance security, each encrypted E_i of BS_i will not be embedded thoroughly in itself or other blocks. Alternatively, each characteristic value of E_i is separated into 2-bit units. Let all the obtained 2-bit units of all E_i's be CD_0, CD_1, …, $CD_{N\times N-1}$. To embed each CD_c into O_t, a secret key K_3 is assigned as the seed of PRNG to randomly generate distinct two-dimensional arrangement sets $D_c=(U_c, V_c)$, where $0\leqq U_c, V_c\leqq N\text{-}1$, and c=0, 1, …, $N\times N$-1. D_c represents the coordinate of the relative pixel in O_t. Each CD_c corresponds to D_c and is embedded into the last two LSBs of the pixel in O_t, respectively. Finally, the stego-image O' is obtained.

2.2. Tamper Detection and Image Restoration Processes

To detect if the image is tampered or not, the first step is to extract the embedded characteristic values from the stego-image O'. The secret key K_3 is used as a seed of PRNG to obtain the two-dimensional arrangement positions (U_c, V_c). The last two LSBs of each pixel at coordinate (U_c, V_c) can be obtained sequentially for an amount of binary data W of $N \times N \times 2$ bits. As a consequence, W has to be decrypted prior to its conversion to the characteristic values.

The encrypted binary data W needs to be decrypted first by applying secret key K_2. PRNG (K_2) is used to produce binary random sequence G of $N \times N \times 2$ bits. Next, G is divided into non-overlapping subsequences G_0, G_1, …, $G_{N\times N\times 2/k-1}$, where each G_b is expressed as k-bit $BG_{b,m}$, m=0, 1, …, k-1. Additionally, binary data W is also divided into W_0, W_1, …,$W_{N\times N\times 2/k-1}$, where each W_b is expressed as k-bit $BW_{b,m}$, m=0, 1, …, k-1. Now according to Equation (7), the logical operation XOR is executed sequentially on each $BG_{b,m}$ and $BW_{b,m}$ to decrypt W_b. Then, the decrypted W_b is converted into decimal data as W_b'. Then, we can use Y converted frequency coefficients to recover a set of characteristic values and each obtained H sets can be associated with a block such that each CV_i'' is sequentially recovered from the stego-image. Each CV_i'' corresponds to block BS_i' in stego-image O'.

$$CB_{b,m} = BW_{b,m} \text{ XOR } BG_{b,m}. \qquad (7)$$

Each restored CV_i'' needs to match up with the characteristic values of BS_i' in the stego-image to tell whether or not BS_i' is definitely tampered. Hence, O' is processed by the proposed embedding process with secret key K_1 to retrieve H sets of characteristic values $\underline{CV_i}''$ from the stego-image.

The proposed tamper detection procedure will sequentially match $\underline{CV_i}''$ and CV_i'' based on each set of characteristic values as a unit. It matches the relative frequency coefficients between the two sets. If both H sets in $\underline{CV_i}''$ and CV_i'' do not have at least one set equal to each other, it means that the corresponding block has been tampered and will need to be restored. However, if at least one of the H sets in $\underline{CV_i}''$ and CV_i'' is equal to each other, it means that the corresponding block has not been tampered. If a block BS_i' is found to be tampered, a correct set of characteristic values from the corresponding characteristic CV_i'' must be chosen to restore BS_i'.

3. Experimental Results

The effectiveness of the proposed tamper proofing and recovery scheme is shown by the following experimental results. Throughout the experiments, our platform was Pentium III 500, 64MB RAM, Windows 2000 Professional operating system, and Java programming language. In our experiments, the original images were three gray-level images "Lena", "License Plate", and "NTIT," all composed of 512 × 512 pixels (as shown in Fig. 1 (a), Fig. 2 (a), and Fig. 3(a), respectively). Our embedding process applied DCT transformation to acquire characteristic values in the original image and used the secret key as a seed in conjunction with the PRNG to randomly embed the characteristic values into the original image. Eventually, the stego-images were obtained (as shown in Fig. 1 (b), Fig. 2 (b) and Fig. 3 (b), respectively).

Fig. 1(c), Fig. 2(c) and Fig. 3(c) are the stego-images tampered to different extents, respectively, in which Fig. 1 (c) focuses on the eye part of "Lena" where the eye part has been filled with the color white by the pencil tool in Adobe Photoshop, Fig. 2 (c) focuses on the number 4 of "License Plate" where the number 4 has been erased by the eraser tool, and Fig. 3 (c) is focuses on the NTIT's mark of "NTIT" where NTIT's mark has been removed by the eraser tool. Fig. 1 (d), Fig. 2 (d) and Fig. 3 (d) show the tampered positions pointed out by the tamper detection method. Fig. 1 (e), Fig. 2 (e) and Fig. 3 (e) are the images restored by the proposed restoration method.

4. Conclusions

More and more digital image data is being applied with respect to digital multimedia. However, digital data is easily tampered without distortion. The main goal of the proposed scheme focuses on proof of integrity and exact restoration and prevents an image from being used by people other than authorized users. More importantly, our scheme will work on other important digital image data such as speeding photos, fingerprint make-outs, and so on.

5. References

[1] J. Fridrich and M.Goljan, "Protection of Digital Images Using Self-Embedding," Symposium on Content Security and Data Hiding in Digital Media, New Jesey Institute of Technology, May 14,1999

[2] G. Friedman, "The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image," IEEE Transactions on Consumer Electronics, vol. 39, pp. 905-910, Nov. 1993.

[3] R. C. Gonzalez and R. E. Woods, Digital Image Processing, Addison Wesley, 1992.

[4] C. Y. Lin and S. F. Chang, "A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation," IEEE Transactions on Circuits and Systems for Video Technology, vol. 11, pp. 153-168, Feb. 2001.

[5] R. L. Rivest, A. Shamir and L. Adleman, “A Method for Obtaining Digital Signatures and Public-key Cryptosystems,” Communications of the ACM, vol. 21, pp. 120-126, Feb. 1996.
[6] B. Schneier, Applied Cryptography, Second Ed., Wiley & Sons, 1996.
[7] M. Schneider and S. F. Chang, “A Robust Image Content Based Digital Signature for Image Authentication,” Proceedings of the International Conference on Image Processing, vol. 3, pp. 227-230, Lausanne, Switzerland, Sept. 1996.
[8] S. Walton, “Image Authentication for a Slippery New Age,” Dr. Dobbe’s Journal, vol. 20, pp. 18-26, pr. 1995.
[9] M. Wu and B. Liu, “Watermarking for Image Authentication, ”Proceedings of the IEEE International Conference on Image Processing, vol. 2, pp. 437-441, Chicago, Illinois, Oct. 1998.
[10] P. Wong, “A Watermark for Image Integrity and Ownership Verification,” Final Program and Proceedings of the IS&T PICS 99, pp. 374-379, Savannah, Georgia, Apr. 1999.
[11] C. R. Yang, M. S. Hwang and Y. L. Tang, “Tampering Double Detection Algorithm,” *Proceedings of the Eighth National Conference on Science and Technology of National Defense*, pp. 165-170, Tao-Yuan, Taiwan, Nov. 1999.

Table 1：Experimental results of the proposed scheme

Performance / Images (512×512)	The PSNR of Stego-image (dB)	Embedding Time (sec)	Detection and Recovery Time (sec)
Lena	47.31	7.43	11.92
License Plate	46.24	8.12	12.33
NTIT	47.54	8.53	13.21

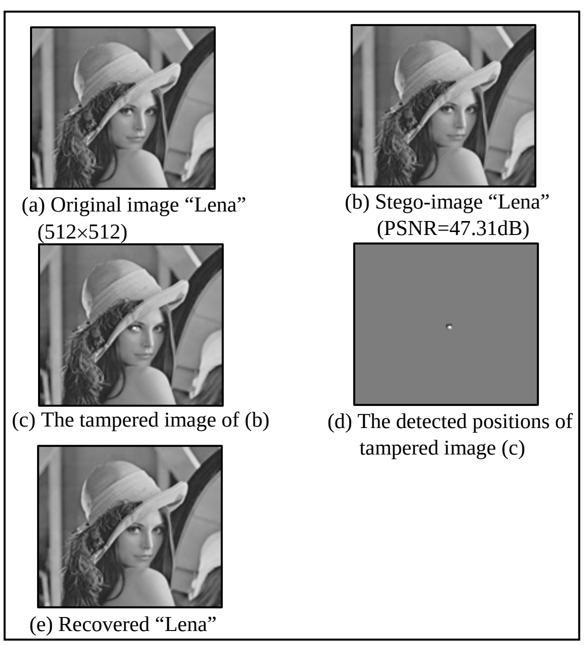
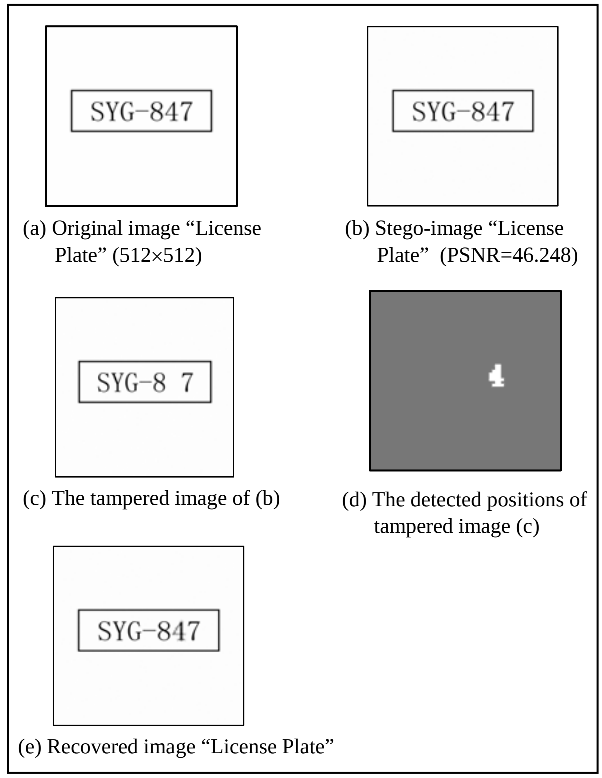

(a) Original image “Lena” (512×512)
(b) Stego-image “Lena” (PSNR=47.31dB)
(c) The tampered image of (b)
(d) The detected positions of tampered image (c)
(e) Recovered “Lena”

Fig. 1: The experimental results of image “Lena”.



(a) Original image “License Plate” (512×512)
(b) Stego-image “License Plate” (PSNR=46.248)
(c) The tampered image of (b)
(d) The detected positions of tampered image (c)
(e) Recovered image “License Plate”

Fig. 2: The experimental results of image “License Plate”.

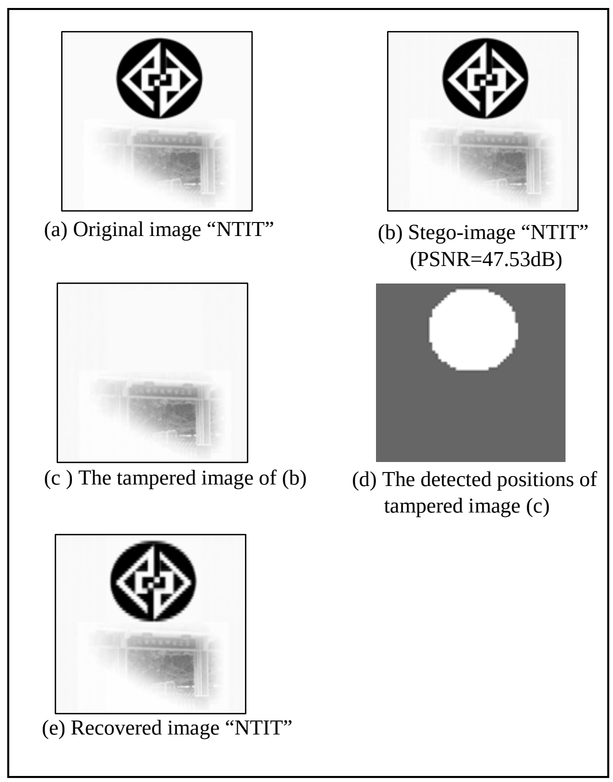

(a) Original image “NTIT”
(b) Stego-image “NTIT” (PSNR=47.53dB)
(c) The tampered image of (b)
(d) The detected positions of tampered image (c)
(e) Recovered image “NTIT”

Fig. 3: The experimental results of image “NTIT”.