International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol.7, No.5 (2014), pp.13-26
http://dx.doi.org/10.14257/ijsip.2014.7.5.02

A Novel Active Image Authentication Scheme for Block Truncation Coding

Chang-Ming Wu[1], Yu-Chen Hu[2], Kuo-Yu Liu[3] and Jun-Chou Chuang[3]

[1]*Department of Electronic Engineering,*
Chung Yuan Christian University, Chung-Li 32023, Taiwan
[2]*Department of Computer Science and Information Management,*
Providence University, 200 Chung Chi Rd., Taichung 43301, Taiwan
[3]*Department of Computer Science and Information Engineering,*
Providence University, 200 Chung Chi Rd., Taichung 43301, Taiwan
cmwu@cycu.edu.tw, {ychu, kyliu, lzchung}@pu.edu.tw

Abstract

In this paper, a simple active image authentication scheme for the compressed images of block truncation coding (BTC) is proposed. In this scheme, the authentication codes of the compressed blocks are generated from the random value induced by the random seed. The authentication code of each compressed block is embedded into the bit map. The bit length of each authentication code can be chosen according to the user's requirement. The experimental results indicate that the proposed scheme detects the tampered areas clearly and keeps good image qualities of the embedded images. Meanwhile, a low computational cost is required in the proposed scheme.

Keywords: *tamper detection, image authentication, and block truncation coding, digital signature, fragile watermarking*

1. Introduction

Recently, the research towards the image tamper detection becomes more and more important because digital images can be easily modified and duplicated by using the computer software. For example, the widely used image processing applications, such as Photoshop and Photo Impact, Painter, and so on, can be used to create image forgeries. The forged image may cause some problems. The public opinion may be misled and the truth in news reports may be distorted due to the forged images. Besides, it is possible that academic papers may contain some forged images that are used to exhibit better experimental results.

These multimedia security issues have led to the design of the image authentication schemes for image tamper detection [1]. The image authentication schemes can be divided into two main categories: passive authentication and active authentication [2], as shown in Figure 1.

Passive image authentication [3-4], which is also called digital image forensics, is the process of authenticating digital images without using any additional information aside from the digital images themselves. These schemes can be either forgery-type dependent or independent. The forgery-type dependent schemes are designed for specific types of forgeries, such as copy-move or image splicing, while the forgery-type independent schemes are designed to detect forgeries regardless of the type of the forgery.

ISSN: 2005-4254 IJSIP

The active image authentication schemes can be classified into two approaches: the signature-based approach [5-6] and the fragile watermark-based approach [7-21]. In the signature-based approach, the given image is processed by using the hash function and the hashed result is encrypted by using the public key cryptosystem to generate the digital signature. Then, the digital signature of the image to be protected is stored in a trust third party. When one given image is to be authenticated, its digital signature is extracted from the trust third party and it is compared to the other signature that is generated from the image to detect the tampered areas.

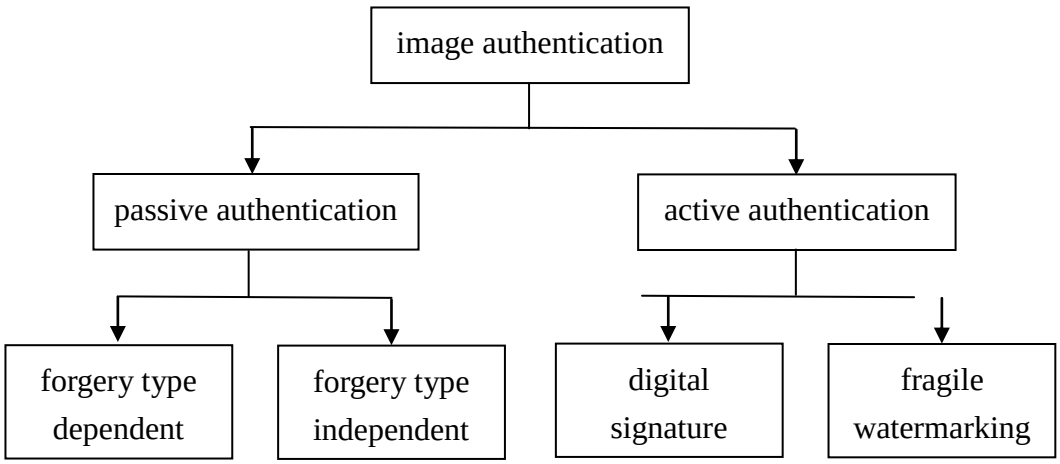


Figure 1. Classifications of the Image Authentication Schemes

In the fragile watermark-based approach, the watermark is often generated by using either the random values induced by the selected random number seed or the image features extracted from the image to be protected. Then, the watermark is embedded into the image to be protected. When the image is to be authenticated, the watermark is extracted from the image to detect the tampered areas.

From the literature, several fragile watermark schemes had been introduced. Lin and Chang proposed a semi-fragile watermarking scheme [7] which can be resistant to lossy compression for JPEG images. In 2003, Tsai, *et al.*, [9] proposed a tamper detection scheme based on SPIHT. Wang and Chen proposed the majority-voting based watermarking scheme for color image [10] in 2007. Lee and Lin proposed the dual watermark for both image tamper detection and image recovery [11] in 2008. Qi and Xin proposed a quantization-based semi-fragile watermarking scheme [12] for image content authentication in 2011.

In addition, Chung and Hu proposed an adaptive image authentication scheme for VQ compressed images [13]. The authentication codes are generated by the random values induced by the specific random seed. Then, the authentication codes embedded into the indices of the compressed images of VQ. Tsai, *et al.*, proposed an image authentication technique for progressive image transmission [14] in 2012. Hu, *et al.*, proposed the tamper detection scheme for BTC-compressed images [15]. In this scheme, 1-bit authentication data is generated from the quantization levels of each image block. Multiple block permutations are generated by using the random sequences induced by the selected random number seeds. Multiple copies of the authenticaiton data are embedded into the bit maps of BTC-compressed image blocks based on the block permutations. In addition, a joint image coding and image authentication scheme based on BTC had been proposed [16]. Hu, *et al.,* proposed a image integrity protection scheme for BTC-compressed images in 2013 [17]. In

this scheme, the authentication data is embedded into the quantization levels of the compressed data. Tsai, *et al.,* proposed an multi-stage encoded image authentication [18]. In this scheme, the image authentication message is extracted from the image content and then embedded into images according to the multi-stage encoding. Chung, *et al.*, proposed the image tamper detection and recovery scheme for grayscale images [19]. In this scheme, the compressed codes of vector quantization are used to recover the tamper areas. A probability-based image authentication scheme for indexed color images had been proposed [20]. Furthermore, a reversible image authentication scheme based on residual histogram shifting had been proposed [21] to protect the image integrity of the grayscale images.

It is known that most of the image authentication schemes work on the raw images. In this paper, we intend to design an image authentication scheme for the compressed images of the block truncation coding scheme [22-30]. The rest of this paper is organized as follows. The review of two BTC-based schemes will be given in Section 2. Section 3 will present the proposed scheme. The experimental results will be discussed in Section 4. Finally, some conclusions will be given in Section 5.

2. Related Work on Block Truncation Coding

BTC [22] was proposed by Delp and Ritchell in 1979 for grayscale image compression. It is also called the moment-preserving block truncation coding (MPBTC) scheme because it preserves the first and second moments of image blocks. Each grayscale image to be processed is divided into a set of non-overlapping image blocks of $n \times n$ pixels. Each $n \times n$ image block can be viewed as an image vector of k dimensions, where $k = n \times n$.

To compress each image block x, the block mean ($\bar{x}$) and the standard deviation (σ) of x are first calculated. If the intensity of one pixel is less than $\bar{x}$, it is classified as the first group. Otherwise, it is classified as the second group. A corresponding bit with value 0 or 1 is stored in the bit map (*BM*) when this pixel is classified as the first group or the second group, respectively.

Two quantization levels a and b are to be generated to represent the pixels in these two groups, respectively. They can be computed according to the following equations:

$$a = \bar{x} - \sigma \times \sqrt{\frac{q}{k-q}}, \text{ and} \tag{1}$$

$$b = \bar{x} + \sigma \times \sqrt{\frac{k-q}{q}}. \tag{2}$$

Here, q stands for the number of pixels whose values are greater than or equal to $\bar{x}$. Each compressed image block forms a trio (a, b, *BM*) where each quantization level is stored in 8 bits.

In addition to MPBTC, the absolute moment block truncation coding (AMBTC) [23] had been proposed to preserve the sample mean and the sample first absolute central moment in 1984. The main difference between AMBTC and MPBTC is the design of the two quantization levels for each image block. The quantization levels a and b for AMBTC can be computed according to the following equations:

$$a = \frac{1}{k-q} \times \sum_{x_i < \bar{x}} x_i, \text{ and} \tag{3}$$

$$b = \frac{1}{q} \times \sum_{x_i \geq \bar{x}} x_i. \tag{4}$$

Basically, BTC has the advantages of achieving high reconstructed image quality and requiring a low computational cost. The major drawback of BTC is that the compression ratio is low. To solve this problem, some BTC-based image coding schemes [24-25] had been proposed to improve the compression ratio. A novel image compression scheme based on AMBTC had been proposed [24]. The quadtree segmentation technique is employed in this scheme to exploit the variable-sized segmentation. In addition, the concept of using visual patterns to reduce the storage cost of the BTC bit plane is incorporated into this scheme. In addition, an improved image compression scheme based on BTC had been proposed [25]. In this scheme, three techniques are employed to cut down the bit rate of moment preserving block truncation coding. They are the two-dimensional prediction technique, the bit map omission technique, and the bit map coding using edge patterns.

In 2008, the fast algorithm for finding the optimal grouping of BTC had been proposed [26]. By using the optimal grouping threshold instead of the block mean value, this scheme can improve the image quality of the compressed image. A near-optimum block truncation coding method [27] had been proposed in 2011. The truncated K-means algorithm and inter-block correlation had been employed in designing it. In addition, Choi proposed the DPCM-based block truncation coding [28] by bit plane modification to improve the image quality of the compressed image.

BTC can also be applied to color image coding. A predictive color image compression scheme based on AMBTC had been proposed [29]. In this scheme, the high correlations among neighboring image blocks are exploited by using the similar block prediction technique. In addition, the bit plane omission technique and the coding of quantization levels are used to cut down the storage cost of smooth blocks and complex blocks, respectively. In addition, a variable-rate color image coding technique based on AMBTC had also been proposed [30]. In this scheme, the quadtree segmentation technique is employed to partition the color image into variable-sized image blocks according to its block activities. Then, the block truncation coding scheme with the bit map omission technique is employed to encode the image blocks.

3. The Proposed Scheme

The goal of the proposed scheme is to protect the image integrity of BTC-compressed images. To achieve the goal, the authentication codes will be embedded into the bit maps of the compressed data. The proposed scheme consists of the authentication codes generation procedure, the authentication codes embedding procedure, and the tamper detection procedure. These procedures are described as follows.

3.1. The Authentication Codes Generation Procedure

Suppose the $W \times H$ image had already been compressed by BTC with the block size of $n \times n$ pixels. A total of $w \times h$ compressed trios of (a, b, BM) where $w = W/n$ and $h = H/n$ were already generated. Let len denote the bit length of the authentication code for each image block. To generate the len-bit authentication code for each compressed image block x, the pseudo random number generator with the predefined seed is used to generate $w \times h$ random values. Each random value rv is converted to the authentication code (ac) of len bits by using the following equation:

$$ac = rv \bmod 2^{len}. \quad (5)$$

Each authentication code will be embedded into the bit map of the corresponding compressed block in the image compression and the authentication data embedding procedure.

An example of authentication code generation is described in the following. Suppose we want to generate 16 authentication codes. First, we need to choose the random seed that is used to induce the random number sequence. Suppose the random seed is set to 2012. The first 16 random values induced by the random seed are listed in Figure 2(a). The corresponding authentication codes of size 1 bit and 2 bits are listed in Figures 2(b) and 2(c), respectively.

6608	6633	17455	19488
19635	15289	11929	8080
5018	14236	3178	18418
12848	31969	8384	2240

(a) Random values

$(0)_2$	$(1)_2$	$(1)_2$	$(0)_2$
$(1)_2$	$(1)_2$	$(1)_2$	$(0)_2$
$(0)_2$	$(0)_2$	$(0)_2$	$(0)_2$
$(0)_2$	$(1)_2$	$(0)_2$	$(0)_2$

(b) 1-bit authentication codes

$(00)_2$	$(01)_2$	$(11)_2$	$(00)_2$
$(11)_2$	$(01)_2$	$(01)_2$	$(00)_2$
$(10)_2$	$(00)_2$	$(10)_2$	$(10)_2$
$(00)_2$	$(01)_2$	$(00)_2$	$(00)_2$

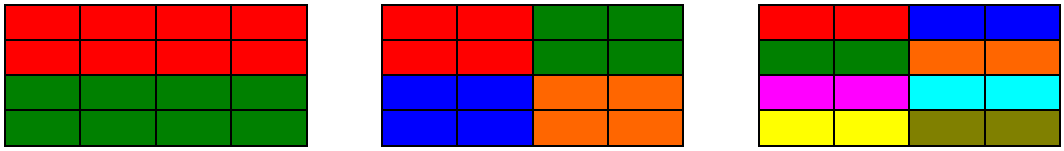
(c) 2-bit authentication codes

Figure 2. Example of Authentication Data Generation

3.2. The Authentication Codes Embedding Procedure

To embed the authentication code *ac* into *BM*, *BM* is divided into *len* equal-sized blocks. An example of bit map division is depicted in Figure 3. In this example, the size of the bit map is 4×4. In these three grouping examples as shown in Figures 3 (a) to 3(c), the *len* values are set to 2, 4, and 8, respectively.

Each sub-divided bit map will be used to embed 1-bit authentication data. The parity value *pv* of each sub-divided bit map is computed. If *pv* equals the 1-bit authentication data, the sub-divided bit map is unchanged. Otherwise, one candidate in the subdivided bit map will be selected and changed so that the parity value of the modified sub-divided bit map will be equal to the 1-bit authentication data. To select the victim, the number of neighbors belonging to the other group for each candidate in the sub-divided bit map is computed. Then, the candidate that has the maximal value is selected for bit map modification.



(a) *len* = 2 (b) *len* = 4 (c) *len* = 8

Figure 3. Example of the Bit Map Division

3.3. The Temper Detection Procedure

To determine whether these *w*×*h* image blocks are tampered or not, two sets of authentication codes are to be generated. The first set of authentication codes is generated by the random values induced by the selected random number seed. A total of *w*×*h* random values are generated. Each random value *rv* is then converted into *eb*-bit authentication code *ac* by using Eq. (5).

The second set of the authentication codes will be generated by using the bit maps. Each bit map of *n*×*n* bits is divided into *len* equal-sized blocks. The parity value of each sub-divided bit map is computed. These parity values of *len* sub-divided bit maps are collected to form the extracted authentication code (*eac*) of each image block.

When two sets of the authentication codes are available, we can determine whether each image block *x* is tampered or not. If *ac* equals *eac*, each image block *x* is classified as a clear

block. Otherwise, *x* is classified as a modified block. By successively processing each block, the roughly detected result is now generated.

The roughly detected result needs to be further refined because it is possible that some modified bit maps may have the same *len*-bit parity values as the original bit maps. The possibility of this condition decreases as the *len* value increases. To improve the detecting accuracy, the tamper refinement process is employed to process the roughly detected image of size *w*×*h*.

(a) Case 1 (b) Case 2 (c) Case 3 (d) Case 4

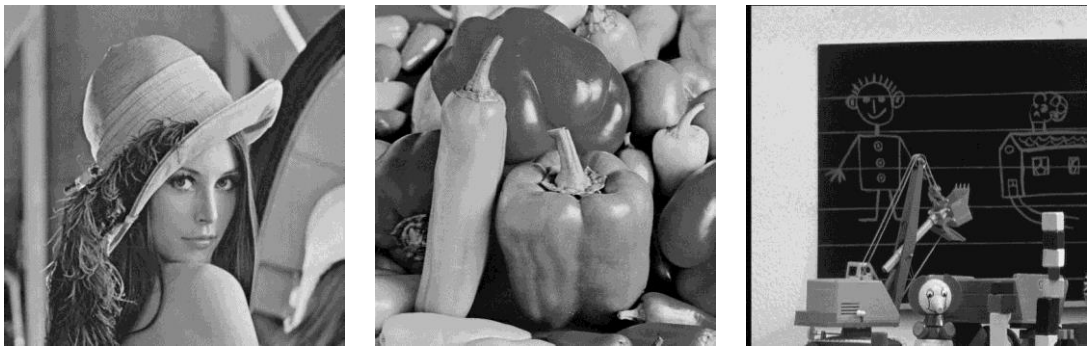
Figure 4. Four Test Cases for Tamper Refinement

Four test cases as shown in Figure 4 are sequentially checked to decide whether each white pixel will be changed to a black one or not. Here, the white pixels and the black pixels stand for the clear and modified blocks, respectively. After checking each white pixel to determine whether it should be changed to a black one or not, the total number of modified pixels in each round is calculated. If the number of modified pixels is greater than or equal to 1, the same refinement process is iterated. Otherwise, the tamper refining process is stopped.

4. Experimental Results

In the simulations, six grayscale images "Airplane", "Girl", "Goldhill", "Lenna", "Peppers", and "Toys" of 512×512 pixels as shown in Figure 5 are used. The size of the image block is set to 4×4. In each test image, there are 16384 image blocks. In the simulations, AMBTC is used as the test method. That is because AMBTC is proved to provide better reconstructed image qualities in terms of squared Euclidean distance.

(a) Airplane (b) Girl (c) Goldhill



(d) Lenna (e) Peppers (f) Toys

Figure 5. Grayscale Testing Images

In the simulations, the peak signal-to-noise-ratio (PSNR) measurement is used. The PNSR measurement is defined as

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} . \quad (6)$$

Here, MSE denotes the mean square error (MSE) between the original and the reconstructed images of $W \times H$. Basically, *PSNR* is considered as an indication of image quality rather than a definitive measurement; however, it is a commonly used measurement for evaluating the image quality.

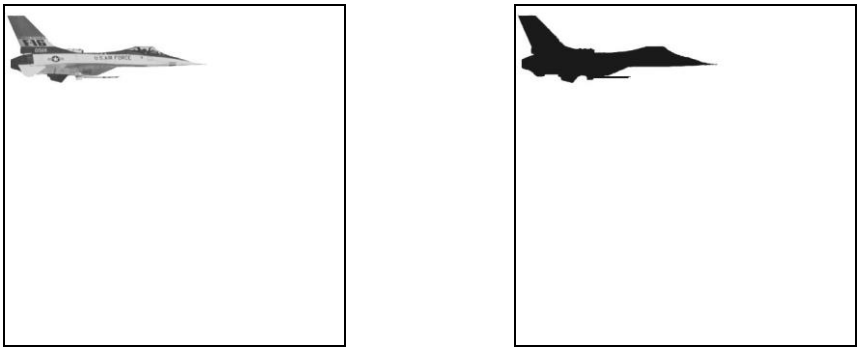
Table 1. Experimental Results of the Image Qualities of AMBTC and the Proposed Scheme

Methods / Images	AMBTC	Proposed Scheme			
		len = 1	*len* = 2	*len* = 3	*len* = 4
Airplane	33.266	31.942	30.710	29.650	28.686
Girl	34.763	33.667	32.298	31.536	30.590
Goldhill	33.694	32.773	31.809	30.981	30.042
Lenna	33.692	33.001	32.193	31.432	30.737
Peppers	34.069	33.239	32.200	31.402	30.473
Toys	33.235	31.248	29.714	28.454	27.422
Average	**33.787**	**32.645**	**31.487**	**30.576**	**29.658**

Image qualities of AMBTC and the proposed scheme are shown in Table 1. Average image quality of 33.787 dB is obtained by AMBTC. It is shown that the image qualities of the proposed scheme decrease as the *len* value increases. Average image qualities of 32.645 dB, 31.487 dB, 30.576 dB and 29.658 dB are achieved by using the proposed scheme when *len* values are set to 1 to 4, respectively. Average image quality losses of 1.141 dB, 2.299 dB, and 3.211 dB are obtained by the proposed scheme when the *len* values are 1, 2 and 3, respectively.

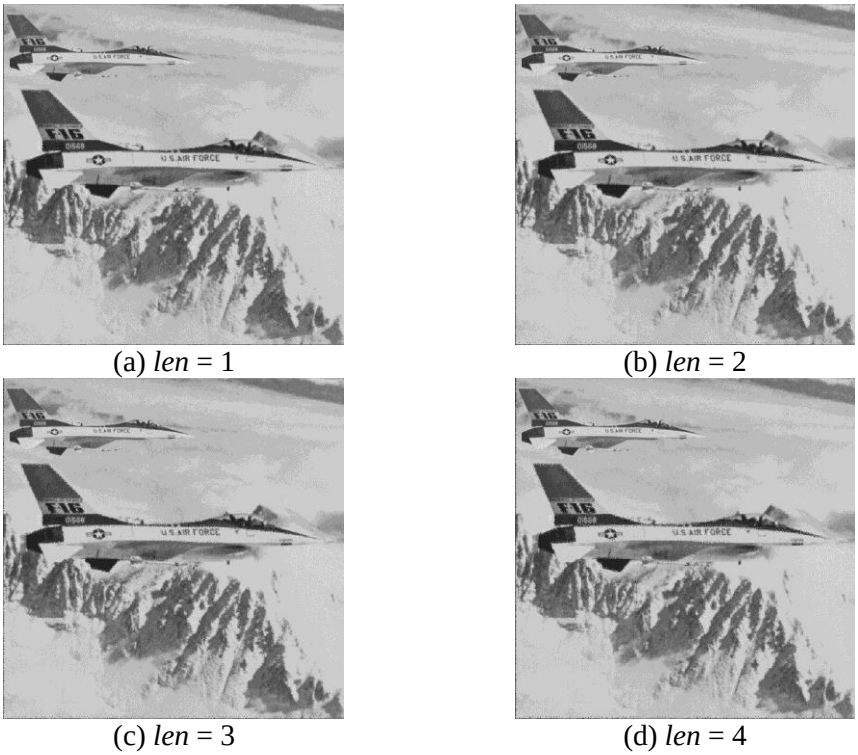
In the tamper test, an airplane as shown in Figure 6(a) is added on the sky of each embedded image. The binary version of the tampered area is shown in Figure 6(b). These four

tampered images when the *len* values are set to 1 to 4 are shown in Figure 7. The tampered object consists of 11002 pixels. A total of 782 blocks are affected by the tampered object.



(a) The tampered object (b) The tampered object in binary form

Figure 6. The Tampered Object of the Test

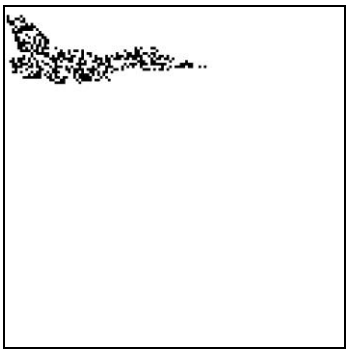


(a) *len* = 1 (b) *len* = 2

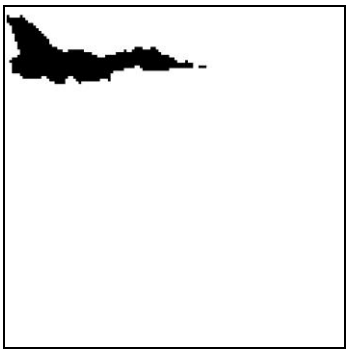
(c) *len* = 3 (d) *len* = 4

Figure 7. Tampered Images of the Embedded Images "Airplane"

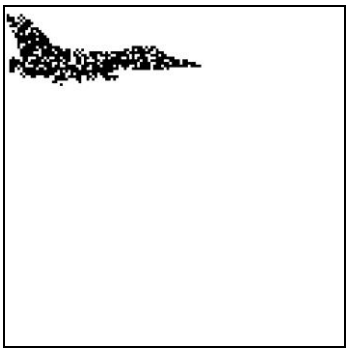
The detected results of the proposed tamper detection procedure are listed in Figure 8. The roughly detected images and the final refined images are listed. Each block spot represents a tampered block in the detected image. The total numbers of the tampered blocks in the roughly detected images and the final refined images of the proposed scheme are listed in Table 2. There are 380, 560, 677 and 703 block spots in the roughly detected images when the *len* values are set to 1 to 4, respectively.



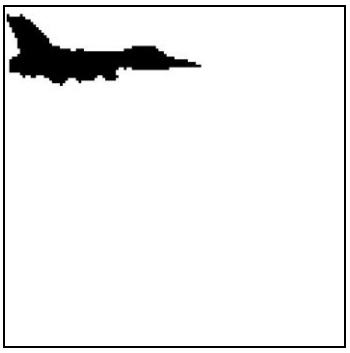
(a) Roughly detected image (*len*=1)



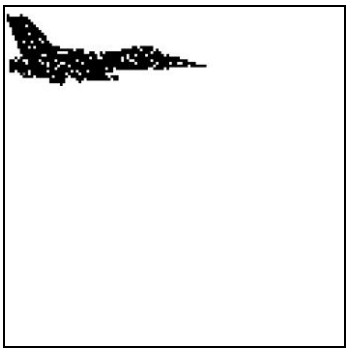
(b) The final detected image (*len*=1)



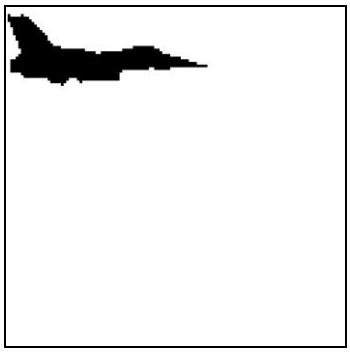
(c) Roughly detected image (*len*=2)



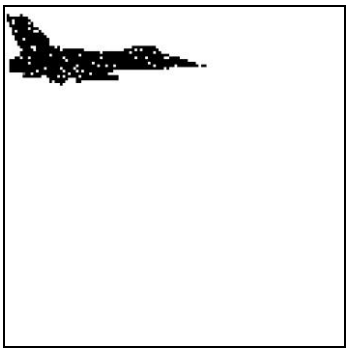
(d) The final detected image (*len*=2)



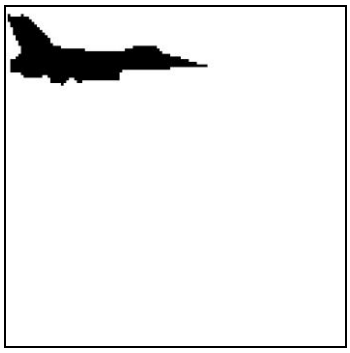
(e) Roughly detected image (*len*=3)



(f) The final detected image (*len*=3)



(g) Roughly detected image (*len*=4)



(h) The final detected image (*len*=4)

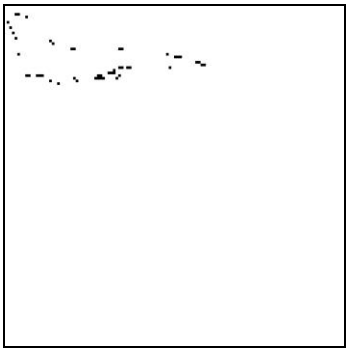
Figure 8. Detected Images of the Proposed Scheme

Table 2. Total Numbers of the Tampered Image Blocks in the Detected Images

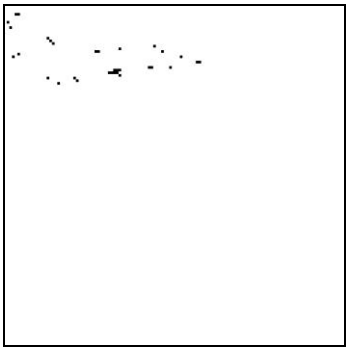
Factors / *len*	Roughly detected image	Final refined image
len = 1	380	704
len = 2	560	744
len = 3	677	768
len = 4	703	771

In the roughly detected image, some tampered blocks cannot be correctly detected because the extracted authentication codes may have the same values with the original ones. According to the roughly detected images, it is shown that the number of black spots increases when the *len* value increases. Compared to the tampered object as shown in Figure 6, the tampered area of each refined image is clearly detected. No white spots are found in the tampered objects in these refined images. But, some tampered blocks in the object boundary cannot be corrected detected.

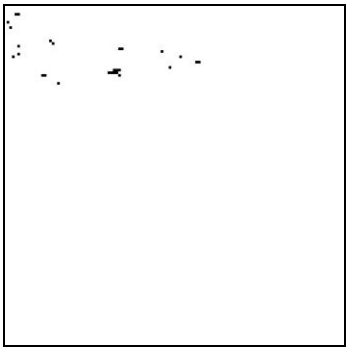
(a) 82 black spots when *len* is set to 1



(b) 48 black spots when *len* is set to 2



(c) 32 black spots when *len* is set to 3



(d) 27 black spots when *len* is set to 4

Figure 9. Results of the False Detection for the Tamper Test

The analysis of the detecting accuracy for these two tamper tests is listed in Table 3. The results of true positive (*TP*), true negative (*TN*), false positive (*FP*), and false negative (*FN*) are provided for these tests. There are 16384 image blocks for each 512×512 image when the block size is set to 4×4. Recall that 782 blocks are affected when an airplane is added into each embedded image in the tamper test.

In the tamper test, 80, 43, 23, and 19 modified blocks are not correctly detected when the *len* values are set to 1 to 4, respectively. According to the false detection images shown in

Figure 9, they exist in the boundary of the tampered object. In addition, 2, 5, 9, and 8 clear blocks are mistakenly detected as modified blocks due to the tamper refinement strategy when the *len* values are set to 1 to 4, respectively. They are also located in the boundary of the tampered object according to the false detection images.

Table 3. Analysis of the Detection Precision of the Temper Tests (Unit: Block)

Factors \ *len*	*len* = 1	*len* = 2	*len* = 3	*len* = 4
TP	15600	15597	15593	15594
TN	2	5	9	8
FP	80	43	23	19
FN	702	739	759	763

Results of the false detected images of the proposed tamper detection procedures are listed in Figure 9. The false detected image blocks are found in the boundary of the tampered area in each refined image. The numbers of the false detected tampered blocks in the refined images are 82, 48, 32, and 27 when the *len* values are set to 1, 2, 3, and 4, respectively.

5. Conclusions

In this paper, a tamper detection scheme that embeds the authentcaiton codes into the bit maps for BTC compressed images is proposed. In the propsed scheme, the authentication codes are generated based on the random values induced by the random number seed. The length of authentication code for each compressed image block can be determined by users to reach a compromise between the embedded image quality and the detection accuracy in the proposed scheme.

According to the results, it is shown that clear tampered areas can be detected. To provide good image qualities of the embedded images, we suggest that the size of the authentication code should be set to 2. The proposed tamper detection scheme can be extended to the image integrity protection for the compressed images that were compressed by the BTC-based image coding technique.

Acknowledgements

This research was partially supported by National Science Council, Taipei, R.O.C. under contract MOST 103-2410-H-126-009-MY3 and MOST 103-2632-E-126-001-MY3.

References

[1] F. Bartolini, A. Tefas, M. Bami and M. I. Pitas, "Image authentication techniques for surveillance applications," Proceedings of IEEE, vol. 89, no. 10, **(2001),** pp. 1403-1418.
[2] S. Lian and D. Kanellopoulos, "Recent advances in multimedia information system security," Informatica, vol. 33, **(2009),** pp. 3–24.
[3] A. Ho, Y. Shi, H. Kim, M. Barni, W. Wang, J. Dong and T. Tan, "A survey of passive image tampering detection," Digital Watermarking, Springer, Berlin/Heidelberg, vol. 5703, **(2009)**, pp. 308-332.
[4] O. M. Al-Qershi and B. E. Khoo, "Passive detection of copy-move forgery in digital images: state-of-the art," Forensic Science International, vol. 231, no. 1-3, **(2013),** pp. 284-295.
[5] L. Xie, G. R. Arce and R. F. Graveman, "Approximate image message authentication codes," IEEE Transactions on Multimedia, vol. 3, no. 2, **(2001),** pp. 242-252.

[6] S. Ababneh, R. Ansari and A. Khokhar, "Iterative compensation schemes for multimedia content authentication," Journal of Visual Communication and Image Representation, vol. 20, no. 5, **(2009),** pp. 303-311.
[7] C. Y. Lin and S. F. Chang, "A robust image authentication method distinguish JPEG compression from malicious manipulation," IEEE Transactions on Circuits and Systems for Video Technology, vol. 11, no. 2, **(2001),** pp. 153-168.
[8] C. Rey and J. L. Dugelay, "A survey of watermarking algorithms for image authentication," EURASIP Journal on Applied Signal Processing, vol. 2002, no. 1, **(2002),** pp. 613–621.
[9] P. Y. Tsai, Y. C. Hu and C. C. Chang, "Using set partitioning in hierarchical trees to authenticate digital images," Signal Processing Image Communication, vol. 18, no. 9, **(2003),** pp. 813-822.
[10] M. S. Wang and W. C. Chen, "A majority-voting based watermarking scheme for color image tamper detection and recovery," Computer Standards & Interfaces, vol. 29, no. 5, **(2007),** pp. 561-570.
[11] T. Y. Lee and S. D. Lin, "Dual watermark for image tamper detection and recovery," Pattern Recognition, vol. 41, no. 11, **(2008),** pp. 3497-3506.
[12] X. Qi and X. Xin, "A quantization-based semi-fragile watermarking scheme for image content authentication," Journal of Visual Communication and Image Representation, vol. 22, no. 2, **(2011),** pp. 187–200.
[13] J. C. Chuang and Y. C. Hu, "An adaptive image authentication scheme for vector quantization compressed image," Journal of Visual Communication and Image Representation, vol. 22, no. 5, **(2011),** pp. 440-449.
[14] P. Y. Tsai, Y. C. Hu, H. L. Yeh and W. K. Shih, "Watermarking for multi-resolution image Authentication," International Journal of Security and Its Applications, vol. 6, no. 2, **(2012)**, pp. 161-166.
[15] Y. C. Hu, W. L. Chen, C. C. Lo and C. M. Wu, "A novel tamper detection scheme for BTC compressed images," Opto-Electronics Review, vol. 21, no. 1, **(2013),** pp. 137-146.
[16] Y. C. Hu, C. C. Lo, W. L. Chen and C. H. Wen, "Joint image coding and image authentication based on AMBTC," Journal of Electronic Imaging, vol. 22, no. 1, **(2013),** art no. 013012.
[17] Y. C. Hu, C. C. Lo, C. M. Wu, W. L. Chen and C. H. Wen, "Probability-based tamper detection scheme for BTC-compressed images based on quantization levels modification," International Journal of Security and Its Applications, vol. 7, no. 3, **(2013),** pp. 11-32.
[18] Y. S. Tsai, P. Y. Tsai and Y. C. Hu, "Watermarking for Multi-stage Encoded Image Authentication," Imaging Science Journal, vol. 61, no. 2, **(2013)**, pp. 65-79.
[19] J. C. Chuang, Y. C. Hu, C. C. Lo and W. L. Chen, "Grayscale image tamper detection and recovery based on vector quantization," International Journal of Security and Its Applications, vol. 7, no. 6, **(2013),** pp. 209-228.
[20] C. C. Lo, Y. C. Hu, W. L. Chen and I. C. Chang, "Probability-based image authentication scheme for indexed color images," Journal of Electronic Imaging, vol. 23, no. 3, (**2014**), art no. 033003.
[21] C. C. Lo and Y. C. Hu, "A novel reversible image authentication scheme for digital images," Signal Processing, vol. 98, **(2014),** pp. 174-185.
[22] E. J. Delp and O. R. Mitchell, "Image compression using block truncation coding," IEEE Transactions on Communications, vol. 27, no. 9, **(1979),** pp. 1335-1342.
[23] M. D. Lema and O. R. Mitchell, "Absolute moment block truncation coding and its application to color image," IEEE Transactions on Communications, vol. 32, no. 10, **(1984),** pp. 1148-1157.
[24] Y. C. Hu, "Low-complexity and low-bit-rate image compression scheme based on AMBTC," Optical Engineering, vol. 42, no. 7, **(2003),** pp. 1964-1975.
[25] Y. C. Hu, "Predictive moment preserving block truncation coding for gray-level image compression," Journal of Electronic Imaging, vol. 13, no. 10, **(2004),** pp. 871-877.
[26] C. C. Tsou, Y. C. Hu and C. C. Chang, "Efficient optimal pixel grouping schemes for AMBTC," Imaging Science Journal, vol. 56, no. 4, **(2008),** pp. 217-231.
[27] Y. Yang, Q. Chen and Y. Wan, "A fast near-optimum block truncation coding method using a truncated K-means algorithm and inter-block correlation," AEU - International Journal of Electronics and Communications, vol. 65, no. 6, **(2011),** pp. 576-581.
[28] K. S. Choi, "Bit plane modification for improving MSE-near optimal DPCM-based block truncation," Digital Signal Processing, vol. 23, no. 4, **(2013),** pp. 1171-1180.
[29] Y. C. Hu, B. H. Su and P. Y. Tsai, "Coluor image coding scheme using absolute moment block truncation coding and block prediction technique," Imaging Science Journal, vol. 56, no. 5, **(2008),** pp. 254-270.
[30] W. L. Chen, Y. C. Hu, K. Y. Liu, C. C. Lo and C. H. Wen, "Variable-rate quadtree-segmented block truncation coding for color image compression," International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 7, no. 1, **(2014)**, pp. 65-76.

Authors

Chang-Ming Wu, he received the B.S. and Ph.D. degrees, all in control and electrical engineering from the National Chiao-Tung University, Taiwan, in 1991 and 2000, respectively. From 2000 to 2007, he worked at Industrial Technology Research Institute, where he was R&D engineer for DSL and DVB-T transceiver and receiver chips. From 2007 to 2010, he was on the faculty of the Department of Computer Science and Information Engineering at the Providence University, Taiwan. Since 2010, he has been with the Department of Electronic Engineering, Chung Yuan Christian University at Taiwan, where he is an assistant professor. His current research interests are in the embedded system, vehicle control network, signal processing, and multivariable control system.

Yu-Chen Hu, he is a professor in the Department of Computer Science and Information Management, Providence University, Sha-Lu, Taiwan. He is a member of ACM and IEEE. Dr. Hu Servers as the Editor-in-Chief of International Journal of Image Processing since 2009. He joints the editorial boards of several other journals including International journal of Security and Its Applications, International Journal of Signal Processing, Image Processing and Pattern Recognition, International Journal of Digital Contents and Applications and so on. His research interests include image and signal processing, data compression, information hiding, and data engineering.

Kuo-Yu Liu, she is an assistant professor in the Department of Computer Science & Communication Engineering at Providence University, Taiwan. He is the deputy director of the CALL research center. His research interests include e-learning technologies and the integration of educational model, game-based learning and cross-media analysis.

Jun-Chou Chuang, she received his PhD. degree in computer science and information engineering from the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan in 2004. Currently, Dr. Chuang is an assistant professor in the Department of Computer Science and Communication Engineering, Providence University, Sha-Lu, Taiwan. His research interests include multimedia security, data hiding, digital watermarking and signal processing.

