Semi-fragile watermarking scheme with discriminating general tampering from collage attack

Yaoran Huo, Hongjie He* and Fan Chen
Sichuan Key Lab of Signal and Information Processing, Southwest Jiaotong University, Chengdu, Sichuan, China
E-mail: hyrchina2012@gmail.com, hjhe@swjtu.edu.cn, fchen@swjtu.edu.cn

***Abstract*—A semi-fragile watermarking scheme is proposed to discriminate general tampering and collage attack in this paper. Five bits watermark data of each block generated are divided into the general tampering watermark (GTW) and collage attack watermark (CAW), which are embedded in the same block and the other blocks to discriminate general tampering and collage attack. The general tampered regions are obtained by the GTW data, and used to define a new collage identification parameter (CIP) combined with the consistency mark of collage attack. If the CIP is less than the given threshold, there are collaged regions in the test image and the CAW data is used to localize the collaged region. This work also discusses the selection of threshold of CIP. Experimental results show that the proposed algorithm improves the tamper detection performance compared to the existing semi-fragile watermarking algorithms and has the ability to discriminate general tampering from collage attack.**

I. INTRODUCTION

With the development of computer and image processing technology, digital images can be forged easily with image processing tools, such as Photoshop [1-2]. The authenticity and integrity of the digital images can not be judged just by the human eyes. More and more researchers focus on the problem how to verify the integrity and authenticity of digital images[3]. The digital authentication watermarking technology, which can achieve detection and localization of the tampered regions, is studied to address this problem[4]. As Semi-fragile watermarking can tolerate content preserving manipulations, such as JPEG (Joint Photographic Experts Group) compression etc., while at the same time detect any manipulation that change the image content, the semi-fragile watermarking [5-6, 8-9] attracts more and more attention.

For the semi-fragile watermarking, security and tamper detection performance are the important performance indexes. In [5, 6], a binary image is regarded as the watermark and embedded in the host image. These two schemes can localize the general tampered region. However, they are vulnerable to collage attack proposed by Fridrich in [7] since the correlation of blocks is not introduced. To improve the ability against collage attack, *Qi et al* [8] embedded the watermark of a block in other blocks and the indexes of mapping blocks for different images are generated by different secret keys. This scheme can resist the collage attack. However, different keys are distributed to different images. It is difficult to manage the secret keys. Liu *et al* [9] adopted the global feature of the image—Zernike Moment to generate the watermark to resist collage attack. The difference value between the extracted and estimated Zernike moments was compared with a threshold to localize the tampered blocks. Depending on the separability of Zernike Moment, if one difference between the estimated and extracted one is larger than the threshold, the corresponding region is tampered. Liu's scheme [9] improves the security. However, the localization accuracy is the block with 24×24 pixels. Meanwhile, PFA(Probability of False Acceptance)[10] of Liu's scheme [9] under collage attack is higher. Hence, the security and tamper detection performance of existing semi-fragile watermarking schemes are dissatisfactory.

On the other hand, several fragile watermarking schemes have been proposed to improve the tamper detection performance under collage attack. The statistical detection model (SDM) proposed in [11, 12] achieves a good performance of tamper detection. However, the superior performance of SDM [11, 12] depends on the larger watermark payload. If the watermark payload is lower, the tamper detection performance becomes worse. The watermark payloads of fragile watermarking schemes [11,12] are about 2 to 3 bpp (bit per pixel), and that of semi-fragile ones is about 0.007 to 0.15 bpp. As a result, the fragile and semi-fragile watermarking cannot be applied directly in the semi-fragile watermarking schemes. Furthermore, the SDM does not have the ability to distinguish whether the detected regions are attacked by the general tampering or the collage attack. This problem might be important to practical application. Anyone can make some modifications on the watermarked images, but not everybody can create a faked watermarked image by the collage attack. This is because the premise for successfully implementing collage attack is to obtain some watermarked images with the same size generated by the same secret key and same watermarking scheme. As a result, the watermarking scheme presents a novel tamper-proofing which provides more information on who modified the image using collage attack if it distinguishes the collage attack from general tampering. Enlightened by the fact that the watermark embedded in the block itself and that embedded in other blocks can localize the general tampered blocks and the collaged region, the semi-fragile watermarking can be proposed combined with two watermarks to improve the performance. The tamper detection performance can be improved compared with the existing schemes using these two watermarks for tamper detection. On the other hand, two watermarks can be used to discriminate general tampering from collage attack.

A semi-fragile watermarking scheme with discriminating general tampering from collage attack is proposed in this work. For each 8×8 image block, the first two watermark bits

(named as GTW) and the rest three watermark bits (named as CAW) are embedded in the block itself and other blocks randomly. At the receiving end, a two-stage detection method is adopted for tamper detection. The GTW data is used to localize the general tampered region in the first stage. Then, a collage identification parameter (CIP) is defined with the detection result of general tampered region and the consistency mark of CAW. The selection of the threshold of the parameter CIP is discussed under different types of attacks and different tamper ratios. If the calculated CIP is lower than the threshold, there are collaged regions in the received image and the collaged regions are localized using CAW data. Experimental results show that the proposed scheme achieves better invisibility and tamper detection performance. A novel tamper-proofing is presented since the proposed scheme can discriminate general tampering from collage attack.

II. Proposed Scheme with Discriminating General Tampering from Collage Attack

The proposed scheme consists of two parts: watermark embedding and extraction, tamper detection.

A. Watermark Embedding and Extraction

The watermark embedding and extraction method in [13] is used to embed and extract the watermark. For each block, there are five bits in the watermark W_i. Where, there are two bits and three bits in GTW and CAW for each block, respectively. With more watermark bits the tamper detection performance will be better. As GTW and CAW are used to detect general tampered region and collaged region respectively, there should be equal watermark bits in GTW and CAW to balance the tamper detection performance under general tampering and collage attack. However, there are five bits totally in W_i and the general tampered region can be detected more easily than the collaged region. As a result, two and three bits are distributed to GTW and CAW. Some symbols should be described clearly. $Y=\{Y_i|\ i=1,2,\ldots,\ N\}$ is the received image and Y_i is 8×8 non-overlapping blocks. $L^g=\{l^g_i\ |\ i=1,2,\ldots,N\}$ and $L^c=\{l^c_i|\ i=1,2,\ldots,N\}$ are the consistency mark of general tampering and that of collage attack. $E_i=\{e_{ik}|\ k=1,2\}$ and $E'_i=\{e'_{ik}|\ k=1,2,3\}$ are the extracted GTW and CAW. $P=\{p_{it}|\ t=1,2,3,\ i=1,2,\ldots,N\}$ is the watermark embedding position.

B. Tamper detection

Our work first uses the GTW to mark the general tampered region. A collage identification parameter (CIP) β is defined according to the localization result and the consistency mark of CAW. If the parameter is less than the threshold, there are tampered regions by collage attack in the received image and the CAW data are used for locating the collaged regions. The steps of tamper detection are shown in Fig.1.

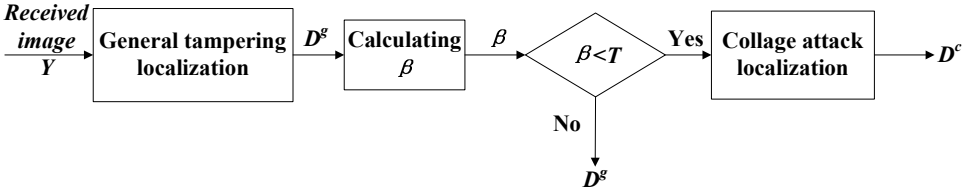

Fig.1 Steps of tamper detection

1) General tampering localization: First, the general tampering consistency mark is processed using the eight neighbor method as shown in (1) and (2). $D\_g1=\{d\_g1_i|\ i=1,\ldots,N\}$.

$$d\_g1_i=\begin{cases}0, if\ d\_g_i=1\ \&\ \sum_z d\_g_z<3\\ d\_g_i, otherwise\end{cases} \tag{1}$$

$$d\_g_i=\begin{cases}1, if\ l^g{}_i=0\ \&\ \sum_z l^g{}_z>3\\ l^g{}_i, otherwise\end{cases} \tag{2}$$

Where, $z\in$ N_8(i). N_8(i) represents the indexes of eight neighbor blocks of Y_i.

Then, the outer boundary blocks are updated by L^g as shown in (3) and the detection result of general tampering $D^g=\{d^g_i|\ i=1,\ldots,N\}$ can be obtained. Where, if $d^g_i=1$, Y_i is tampered under general tampering. Otherwise, Y_i is authentic or collage attacked.

$$d^g{}_i=\begin{cases}l^g{}_i, if\ c_i=1\\ d\_g1_i, otherwise\end{cases} \tag{3}$$

Where, $C=\{c_i|\ i=1,\ldots,N\}$.

$$C=imdilate\left(D\_g1, A\right)-D\_g1 \tag{4}$$

The *imdilate*() is dilation operation. A is the structural element of size 3×3.

2) Collage attack localization: To localize the collage attacked region, the CIP β compared with a threshold T is defined to judge whether there is tampered region under collage attack. First, the collage attack parameter β is defined as the followed (5). And β is calculated with the number of all blocks, number of marked blocks in the first stage, the number of blocks whose watermarks are all embedded in the tampered region of D^g and the number of inconsistent blocks whose corresponding watermark is not embedded in the tampered region of D^g.

$$\beta=-\log 2\left(\frac{\sum_i h_i}{N-\sum_i d^g{}_i-\sum_i g'{}_i}\right) \tag{5}$$

Where,

$$h_i=\begin{cases}1, if\ d^g{}_i=0\ \&\ l^c{}_i=1\ \&\ \sum_t g_{it}\neq 0\ \&\ \sum_t d^g{}_{p_{it}}\neq 3\\ 0, otherwise\end{cases} \quad (6)$$

$$g_{it}=\begin{cases}1, if\ d^g{}_{p_{it}}=0\ \&\ e'_{it}\neq e_{it}\\ 0, otherwise\end{cases} \quad (7)$$

$$g'_i=\begin{cases}1, if\ \sum_t d^g{}_{p_{it}}=3\\ 0, otherwise\end{cases} \quad (8)$$

For a given threshold T (the value of T will be discussed in next section), if $\beta<T$, there is forged area by the collage attack in the test image and the followed steps should be implemented to localize the collage attacked region. Otherwise, there is no forged region under collage attack. Then, the program stops and the output detection result is D^g. The tamper detection of collage attack is shown in the followed steps.

a) Tamper mark: The tampered blocks are localized by the tamper map L^c, D^g and the neighborhood method. $U=\{u_i|\ i=1,\ldots,N\}$ is the tamper map.

$$u_i=\begin{cases}0, if\ d^g{}_i=0\ \&\ l^c{}_i=1\ \&\\ \quad \sum_z l^c{}_z<\min\left(\sum_{N\_8(p_{it})} l^c{}_{N\_8(p_{it})}, t=1,2,3\right)\\ l^c{}_i, if\ d^g{}_i=0\ \&\ l^c{}_i=1\ \&\\ \quad \sum_z l^c{}_z\geq\max\left(\sum_{N\_8(p_{it})} l^c{}_{N\_8(p_{it})}, t=1,2,3\right)\\ 1, otherwise\end{cases} \quad (9)$$

Where, $z\in$N_8(i), $z'\in$N_8(p_{it})(t=1,2,3). N_8(i) represents the indexes of eight neighbor blocks of Y_i. min() returns the smallest number. Then, $U^*=\{u^*{}_i|\ i=1,\ldots,N\}$.

$$u^*{}_i=\begin{cases}1, if\ u_i=0\ \&\ \sum_z u_z\geq 4\\ 0, if\ u_i=1\ \&\ \sum_z u_z\leq 3\end{cases} \quad (10)$$

b) Boundary optimization: The boundary of the tampered area $Out=\{out_i|\ i=1,\ldots,N\}$ is firstly extracted. U^* is optimized by L^c and Out.

$$Out=imdilate(U^*,A)-U^* \quad (11)$$

$$u^*{}_i=\begin{cases}l^c{}_i, if\ out_i=1\\ u^*{}_i, otherwise\end{cases} \quad (12)$$

c) Post processing: Processed by above steps, the tampered area under collage attack has been localized. Then, $D^c=\{d^c{}_i|\ i=1,2,\ldots,N\}$is marked as tamper map of collage attacked area shown in (13). Where, if $d^c{}_i=1$, Y_i is tampered under collage attack. Otherwise, it is authenticated or general tampered.

$$d^c{}_i=\begin{cases}1, if\ u^*{}_i=1\ \&\ d^g{}_i=0\\ 0, otherwise\end{cases} \quad (13)$$

After this stage, the final detection result is $D=\{d_i|\ i=1,2,\ldots,N\}$ including result of general tampered region and that of collage attack.

$$d_i=\begin{cases}1, if\ u^*{}_i=1\ or\ d^g{}_i=1\\ 0, otherwise\end{cases} \quad (14)$$

If d_i=1, Y_i is tampered by general tampering or collage attack. Otherwise, it is authentic. Where, localization results of general tampered and collage attacked regions are D^g and D^c, respectively.

III. Experimental Results

To show the effectiveness of the proposed scheme, kinds of experiments using the proposed scheme, [5], [6], [8] and [9] are implemented, including invisibility, semi-fragility under JPEG, selection of the threshold T and tamper detection performance. The invisibility is measured by PSNR and semi fragility against JPEG compression is measured by bit error rate (BER). And the PFA (denoted as P_{FA}), PFR (Probability of false rejection, denoted as P_{FR}) and PFD(Probability of false decision) in [10] are used to evaluate the tamper detection performance. The test images are of size 512×512. The thresholds in [9], T_1 and T_2 are 3320 and 512 respectively. The step size for dither in [5] is 15. In [8], the quantizer is 15. In this section, the collage attack proposed in [7] is used for experiments. Two watermarked images are used to implement the collage attack. These two watermarked images are of the same size and watermarked by the same watermarking scheme using the same keys. Then one region in one watermarked image is pasted on the same location of the same size of the other watermarked image.

A. Invisibility

Thirty test images, which are rough or smooth, are used to show the invisibility of the proposed scheme, [5], [6], [8] and [9]. In [6], intensity factor is 0.08. The quality factor in the proposed scheme is 70. The watermark payload of the proposed scheme, [5], [6], [8] and [9] are 0.07bpp (bit per pixel), 0.007bpp, 0.11bpp, 0.06bpp and 0.015bpp. The statistical results are shown in Fig.2. As shown in Fig.2, PSNR of the proposed scheme is about 44dB which is acceptable. And the PSNR of the proposed scheme is higher than [5], [6], [8] and [9]. Although watermark payloads of the scheme [8] and [9] are lower, [8] and [9] embedded the watermark in the LL band which contains the main power of the image. Then, the invisibilities of [5], [8] and [9] are lower. As the scheme in [6] embeds the watermark in the spatial domain, PSNR of [6] closely relates to the roughness of the images and the PSNR fluctuates strongly. In the ninth point of the line [6], the image is so smooth that the PSNR of [6] is higher than the proposed scheme. In conclusion, invisibility of the proposed scheme is better than [5, 6, 8, 9] generally.

B. Semi-fragility under JPEG compression

To show the semi-fragility under JPEG of the proposed scheme, BER(bit error rate) of the extracted watermark and the embedded watermark is used. The given quality factor is 70. As shown in TABLE I, the proposed scheme can resist JPEG

compression of which the quality factor is higher than the given one.

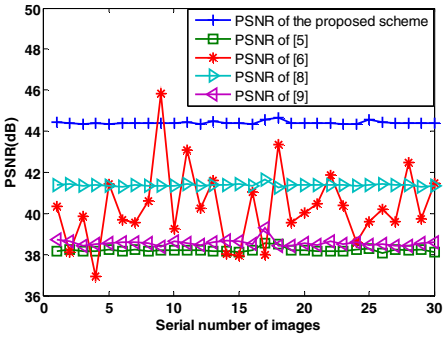

Fig.2 PSNR of the proposed scheme, [5], [6], [8] and [9]

TABLE I
BER UNDER JPEG COMPRESSION

Q / *BER*(%)	100	90	80	70	60	50
Lena	0	0	0.078	0	15.56	39.67
Barb	0	0.009	0.006	0	19.64	35.85
Lax	0.004	0.019	0.049	0.004	20.35	36.49
Lake	0	0	0.05	0	17.7	39.4

C. Time Complexity

To show the time complexity of the schemes, Fig.3 shows the time complexity of watermark embedding by the proposed scheme, [5], [6], [8] and [9]. Fifteen images of size 512×512 are used for test. The experiments are implemented on the DELL computer. The CPU(Central Processing Unit) frequency is 2.7GHz, and the RAM(Random Access Memory) is 4G. As seen from Fig.3, the time complexity of the proposed scheme about 2s(seconds) is higher than that of [5] which is about 0.07s. However, the time complexity of [6], [8] and [9] is higher than the proposed scheme.

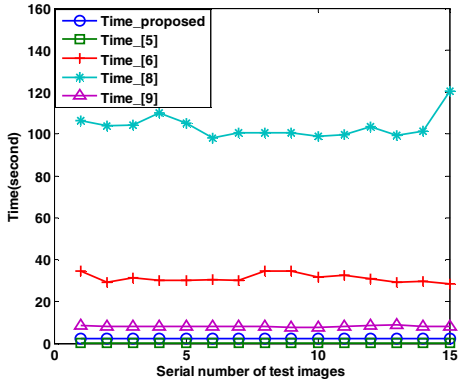

Fig.3 Time complexity of several images

D. Selection of the threshold T

In this subsection, the images-'Bridge', 'Lake' and 'Baboon' are used to statistic the collage identification parameter (CIP) β under general tampering, collage attack and hybrid attack. The tamper ratio of general tampering and collage attack is from 1% to 96% and the tampered blocks are selected randomly. The experimental results are shown in Fig.4. For hybrid attack consisting general tampering and collage attack, the image 'Baboon' is tested. The general tamper ratios are selected as 29%, 58% and 87% and the tampered blocks under collage attack is selected from the rest blocks.

As shown in Fig.4, under general tampering, β>5. Under collage attack, β<4. Under hybrid attack, β<4.5. As a result, [4.5, 5] is the interval which can be used to select *T*. Then, in this paper, *T* is selected as 4.75.

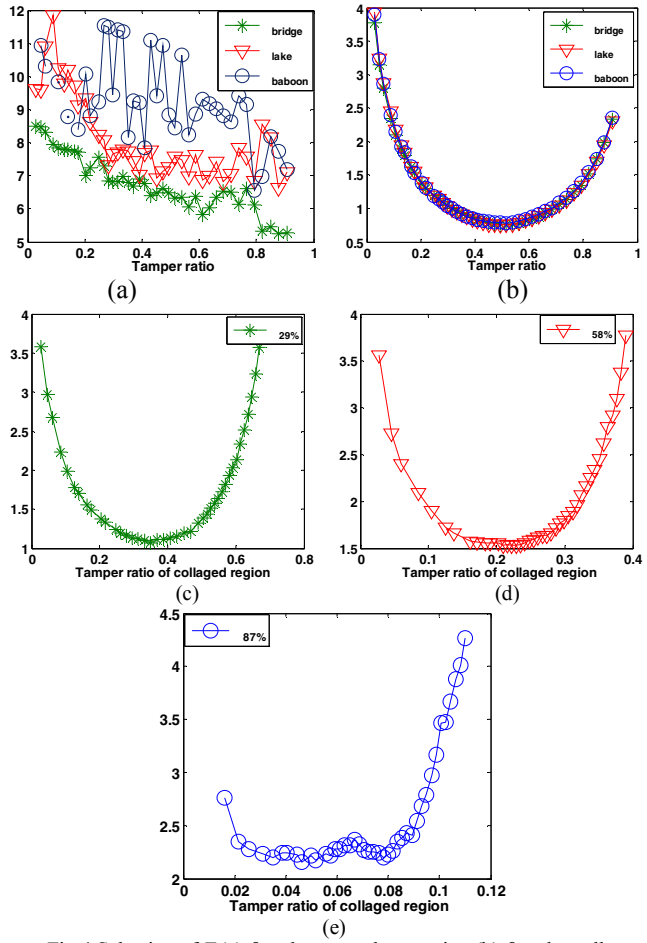

Fig.4 Selection of *T* (a) β under general tampering (b) β under collage attack (c)-(e) β under hybrid attack with the tamper ratio under general tampering 29%, 58% and 87%

E. Tamper detection performance

In this section, PFA, PFR and PFD in [10] are used to evaluate the tamper detection performance of the proposed scheme, [5], [6] [8] and [9] under general tampering, collage attack and hybrid attack. For justice, PFA, PFR and PFD are calculated in pixel for these schemes.

First, in order to show the advantage of the proposed scheme under general tampering, the statistical results of PFD are calculated using the test images-Lena, Baboon, Lake and Lax. PFD indicates the comprehensive change trends of PFA and PFR. Results are shown in Fig.5. For each image, the tampering ratio is from 0.008 to 0.96. Under each tampering ratio, fifty tampered regions are selected randomly and PFD is the average value. In Fig.5, the results are the average value of PFD of those four images under each tampering ratio. As seen from Fig.5, it can be concluded that statistical PFD of the proposed scheme is much lower than the schemes in [5,6,8,9].

That is to say that the proposed scheme improves the tamper detection performance under general tampering.

Above are the statistical results. Here are the specific visual results of Barb under general tampering. The image 'Barb' is used for experiment and the experimental results are shown in Fig.6. The watermarked image, tampered image, and detection results of the proposed scheme, [5], [6], [8] and [9] are shown in Fig.6 (a)-(g). The tamper ratio is 45.2%. The white pixels are tampered pixels. PFA and PFR are calculated in pixel and shown in TABLE II. As shown in Fig.6 (d) to (g) there are many tampered pixels which can not be localized. And almost all the tampered pixels are localized in Fig.6 (c). As shown in TABLE II, the PFA of the proposed scheme is better than [5], [6], [8] and [9] and PFR is a litter higher. However, PFD, which is the weighted sum of PFA and PFR, of the proposed scheme, [5], [6], [8] and [9] are 3.54%, 13.16%, 24.36%, 22.83% and 12.49%. In a word, tamper detection performance of the proposed scheme is better than other schemes. Meanwhile, the calculated β of proposed is 7.138 which is larger than 4.75. Then, the detection result in Fig.6(c) is marked general tampered area. There is no collaged region. In a word, the proposed scheme improves the tamper detection performance under general tampering.

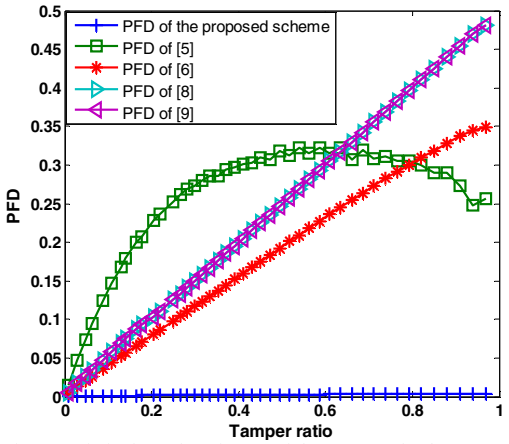

Fig.5 Statistical results of PFD of the proposed scheme, [5], [6], [8] and [9] under general tampering

On the other hand, in the received image there may be tampered regions under general tampering and collage attack simultaneously. Then, the experimental results of hybrid attack consisting of general tampering and collage attack are implemented. The images 'Road' and 'Old' are used for experiments. The tampered region under general tampering is adding some letters on the image 'Road'. The collaged one is pasting the man in watermarked 'Old' into watermarked 'Road'. The tampered image is show in Fig.7(c). Fig.7 (d)-(h) is the detection results of the proposed scheme, [5], [6], [8] and [9]. In Fig.7 (d), the red region is general tampered region and the green region is the collaged area marked by the proposed scheme. Tamper ratio is 9.0% and white pixels are tampered pixels. The schemes in [5], [6], [8] and [9] can not localize the collaged region. The PFA of these schemes are higher. PFD, which is the weighted sum of PFA and PFR, of the proposed scheme, [5], [6], [8] and [9] are 7.37%, 8.99%, 9.03%, 8.97% and 10.16%. The proposed scheme can locate the tampered region under collage attack and general tampering accurately. Meanwhile, the proposed scheme discriminates the general tampering from collage attack. As shown in TABLE II, the detection performance of the proposed scheme is better than [5], [6] [8] and [9]. As the localization unit is 8×8 block and the PFR is calculated in pixel, PFR of the proposed scheme is higher than other schemes as shown in TABLE II. However, the PFD of the proposed scheme is much lower than other schemes.

As seen from above experimental results, the proposed scheme improves the tamper detection performance with better invisibility compared to the semi-fragile watermarking schemes in [5, 6, 8, 9] and can discriminate general tampering from collage attack.

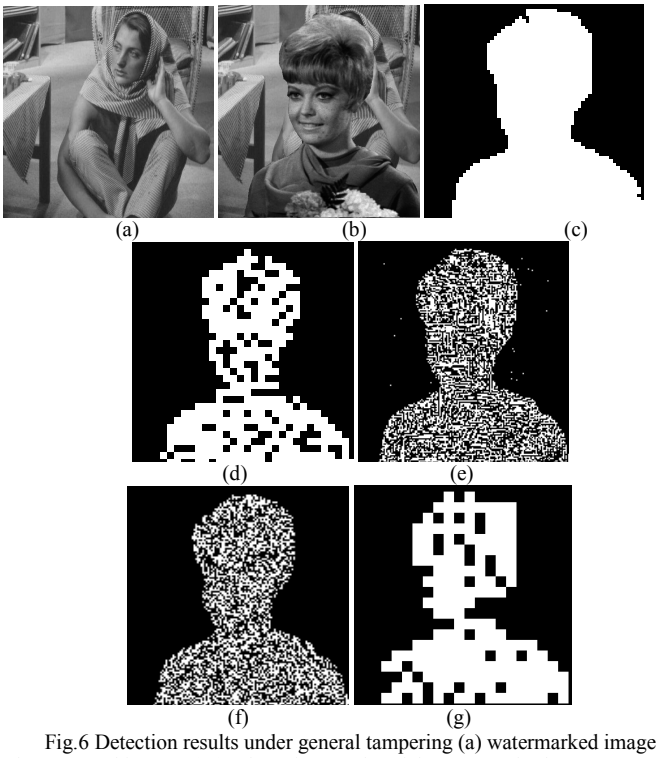

Fig.6 Detection results under general tampering (a) watermarked image (b) tampered image (c)-(g) detection results of the proposed scheme, [5], [6], [8] and [9]

IV. CONCLUSION

This paper proposes a semi-fragile watermarking scheme with discriminating general tampering from collage attack, which presents a new tamper-proofing providing more information on who modified the image. For each 8×8 image block, five bits of watermark consisting of GTW and CAW data are generated by the quantized DCT coefficients. To discriminate general tampering from collage attack, GTW and CAW are embedded in the same block and the other blocks randomly by the secret key respectively. To improve the tamper detection performance, the GTW data is used to localize the tampered region under general tampering firstly. With the localization result in first stage and the consistency mark of CAW, a collage identification parameter (CIP) is defined and the selection of the threshold for the parameter

CIP is discussed in different types of attacks and different tamper ratios. If there are collaged regions in the test image by comparing the parameter CIP with the threshold, the CAW data are used for localizing the collaged region. Experimental results show that the proposed scheme has a superior performance of tamper detection and an ability of discriminating general tampering from collage attack. The future work is to recover the tampered region.

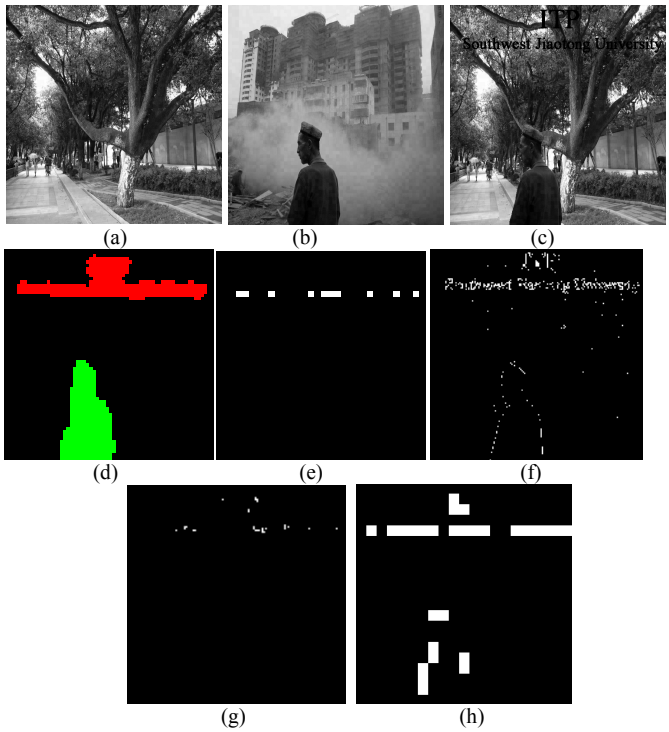

Fig.7 Detection results under hybrid attack (a) watermarked 'Road' (b) watermarked 'Old' (c) tampered image (d)-(h) detection results of the proposed scheme, [5], [6], [8] and [9]

ACKNOWLEDGMENT

This work is supported in part by the National Natural Science Foundation of China (Grant No. 61373180, 61170226), and by the Fundamental Research Funds for the Central Universities (Grant No.SWJTU09CX039, SWJTU10CX09).

REFERENCES

[1] D. Bhattacharyya, T. H. Kim, and G. S. Lee, "Watermarking Using Multi-resolution Cosine Transformation: A Review," Proceedings of international conference on Communications in Computer and Information Science, Springer Press, vol. 260, Dec. 2011, pp. 260: 126-139.

[2] S. H. Han, C. H. Chu, "Content-based image authentication: current status, issues, and challenges," International Journal of Information Security, vol. 9, 2010, pp. 19–32.

[3] A. Trémeau, D. Muselet. "Recent Trends in Color Image Watermarking," Journal of Imaging Science and Technology, vol. 53, Feb. 2009, pp. 010201-010201-15.

[4] A. Haouzia, R. Noumeir, "Methods for image authentication: a survey," Multimedia Tools and Applications, vol. 39, 2008, pp. 1-46.

[5] A. Phadikar, S. Maity, M. Mandal, "Novel wavelet-based QIM data hiding technique for tamper detection and correction of digital images," Journal of Visual Communication & Image Representation, vol. 23, Apr. 2012, pp. 454-466.

[6] W. Zhang, Y. Frank, "Semi-fragile spatial watermarking based on local binary pattern operators," Optics Communications, vol.284, Aug. 2011, pp. 3904-3912.

[7] J. Fridrich, M. Goljan, N. Memon, "Cryptanalysis of the Yeung-Mintzer fragile watermarking technique," Journal of Electronic Imaging, vol.11, Apr. 2002, pp. 262-274.

[8] X. Qi, X. Xin, "A quantization-based semi-fragile watermarking scheme for image content authentication," Journal of Visual Communication and Image Representation, vol. 22, Feb. 2011, pp. 187-200.

[9] H. M. Liu, X. Z. Yao, J. W. Huang, "Semi-Fragile Zernike Moment-Based Image Watermarking for Authentication," EURASIP Journal on Advances in Signal Processing, vol. 2010, 2012, pp. 341856-17.

[10] H. J. He, J. S. Zhang, H. M. Tai, "A wavelet-based fragile watermarking scheme for secure image authentication", Proceedings of 5th International Workshop on Digital Watermarking, Springer Press, vol. 4283, Nov. 2006, pp. 422-432.

[11] H. J. He, F. Chen, H. M. Tai, Ton Kalker, J. S. Zhang, "Performance Analysis of a Block-Neighborhood-Based Self-Recovery Fragile Watermarking Scheme," IEEE Transactions on Information Forensics and Security, vol. 7, Feb. 2012, pp. 185-196.

[12] H. J. He, J. S. Zhang, H. M. Tai, "A neighborhood-characteristic-based detection model for statistical fragile watermarking with localization," Multimedia Tools and Applications, vol. 52, Jan. 2011, pp. 307-324.

[13] Y. R. Huo, H. J. He, F. Chen, "A semi-fragile watermarking algorithm with two-stage detection," Multimedia Tools and Applications, Jan. 2013, online first.

TABLE II
TAMPER DETECTION PERFORMANCE

Detection performance (%)	Tamper ratio (%)	Proposed		[5]		[6]		[8]		[9]	
		P_{FA}	P_{FR}	P_{FA}	P_{FR}	P_{FA}	P_{FR}	P_{FA}	P_{FR}	P_{FA}	P_{FR}
General tampering	45.2	0.2	6.3	27.3	1.5	53.0	0.73	49.7	0.67	22.3	4.4
Hybrid attack	9.0	0	8.1	94.8	0.5	91.9	0.83	98.9	0.08	72.5	4.0