Multimed Tools Appl
DOI 10.1007/s11042-015-2449-0

Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes

Wu-Chih Hu · Wei-Hao Chen · Deng-Yuan Huang · Ching-Yu Yang

Received: 30 June 2014 / Revised: 4 November 2014 / Accepted: 2 January 2015

Abstract This paper proposes an effective image forgery detection scheme that identifies a tampered foreground or background image using image watermarking and alpha mattes. In the proposed method, component-hue-difference-based spectral matting is used to obtain the foreground and background images based on the obtained alpha matte. Next, image watermarking based on the discrete wavelet transform, discrete cosine transform, and singular value decomposition is used to embed two different watermarks into the foreground and background images, respectively. Finally, the difference between the obtained singular values is used to detect tampering of foreground or background image. Experimental results show that the proposed method performs well in terms of image forgery detection.

Keywords Image forgery · Image matting · Image watermarking · Alpha matte

1 Introduction

Digital cameras become cheap and dominating devices in recent years, thus digital images are common in our daily lives. Furthermore, the Internet is in widespread use, so digital images are easy to acquire through the Internet. Therefore, digital images have become ubiquitous. With the availability of powerful image processing technology and digital image editing tools, digital images have become easier to duplicate and manipulate without degrading quality or

W.-C. Hu (✉) · W.-H. Chen · C.-Y. Yang
Department of Computer Science and Information Engineering, National Penghu University of Science and Technology, Magong City, Taiwan
e-mail: wchu@npu.edu.tw

W.-H. Chen
e-mail: a6803072@hotmail.com

C.-Y. Yang
e-mail: chingyu@npu.edu.tw

D.-Y. Huang
Department of Electrical Engineering, Dayeh University, Changhua, Taiwan
e-mail: kevin@mail.dyu.edu.tw

Published online: 14 January 2015

leaving obvious visual clues. Abusive use of image forgery has become a serious problem, and thus the authentication of images has become increasingly important. Therefore, it is a challenging task to obtain accurate and robust detection of image forgery.

Existing technologies for image forensics can be roughly divided into two categories, namely active and passive technologies. The active forensic approach is a non-blind approach, which extracts prior inserted information from a digital image (e.g., digital watermarks or signatures) to determine authenticity. If the embedded information has changed, the image is recognized having been tampered. Image watermarking [7, 8, 22] is a popular active technique. Image watermarking embeds a hidden watermark at recording time and extracts it later to verify image authenticity.

The passive forensic approach is a blind approach with no supplementary information used. That is, blind approaches determine the feature consistency of the image without the use of embedded information. Region duplication detection, a common type of image forgery detection, includes copy-move forgery detection [3, 14, 19] and tampering detection of composite images [1, 20, 24].

Compared to active forensic approaches, passive ones can authenticate an image without any a priori knowledge, making them more practical. However, passive forensic approaches do not work well on images composed of a new background image and an extracted foreground object, with the alpha matte obtained by image matting, as shown in Fig. 1. For instance, copy-move forgery detection does not work well on above composite image. Furthermore, tampering detection of composite images based on the feature consistency of the image does not obtain the accurate result of above composite image.

Image matting is the process of extracting the foreground object from an image along with an opacity estimate for each pixel covered by the object. Although image matting has been studied for more than two decades, image matting has received increasing attention in the last decade and many methods have been proposed for image matting [27]. The state-of-the-art matting algorithms were proposed in the recent years, such as easy matting [6], closed-form matting [17], spectral matting [18], and modified spectral matting [11, 12].

Using image matting can obtain a more realistic image composition using of the new background image and the extracted foreground object with the obtained alpha matte. That is, image composition of a new background image and an extracted foreground object with the obtained alpha matte. Passive forensic approaches (copy-move forgery detection [3, 14, 19] and tampering detection of composite images [1, 20, 24]) do not work well for identifying

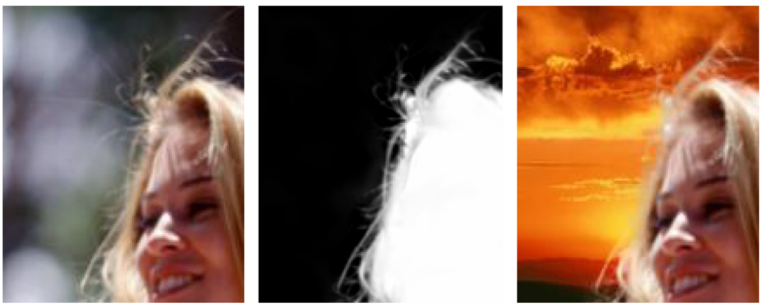

Fig. 1 Example of composite image created using image matting. **a** Original image, **b** alpha matte, and (**c**) tampered image

exchange foreground images or exchange background images. Compared to the passive forensic approach, the active forensic approach is usually used to authenticate a whole image, so it is unsuitable for detecting image forgery in images with a tampered foreground or background. Although recovery of tampered regions using image watermarking were suggested [7, 22], these methods are not robust to the image compression. Therefore, the applications on detection of tampered images are restricted by using these methods.

The present study proposes an image forgery detection scheme that effectively identifies a tampered foreground or background image using image watermarking and alpha mattes. This paper is the modified and extended version of our previous work [9] to greatly increase the performance. Only an exchanged foreground or background image could be detected in our previous work [9]. Furthermore, the used thresholds are given by users, thus it would not be suitable for practical applications. The proposed method in this paper can not only detect an exchanged foreground or background image, it can also detect a tampered foreground or background image with adaptive thresholds. Discrete wavelet transform (DWT)-discrete cosine transform (DCT)-singular value decomposition (SVD)-based image watermarking [10] is used to embed two different watermarks into the foreground and background images, respectively. The foreground and background images are obtained based on the alpha matte using component-hue-difference-based spectral matting [11]. Finally, the difference between the obtained singular values is used to detect tampering of the foreground or background image. Experimental results show that the proposed method performs well in terms of image forgery detection.

The rest of this paper is organized as follows. The proposed image forgery detection scheme is described in Section 2. Section 3 presents experimental results and their evaluations. Finally, conclusions are given in Section 4.

2 Image forgery detection of tampered foreground or background image

In the proposed image forgery detection scheme, DWT-DCT-SVD-based image watermarking [10] and component-hue-difference-based spectral matting [11] are used for watermark embedding and alpha matting, respectively. Before describing the proposed image forgery detection, the DWT-DCT-SVD-based image watermarking and component-hue-difference-based spectral matting are briefly described as below.

2.1 Watermark embedding

DWT-DCT-SVD-based image watermarking has been shown to be robust against rotation, Gaussian noise addition, and JPEG compression attacks [10]. Therefore, the DWT-DCT-SVD-based image watermarking is used to embed the watermarks in the proposed image forgery detection.

In DWT-DCT-SVD-based image watermarking, the cover image is transformed from the RGB color space into the YCbCr color space to obtain a gray-level image. The DWT is then applied to the gray-level image to obtain the LL subband image. The DCT is then applied to the LL subband image to obtain the frequency components. Finally, SVD is used on the obtained frequency components.

In the proposed image forgery detection, only the watermark embedding of the DWT-DCT-SVD-based image watermarking is used and the watermark extraction is not applied. Therefore, this subsection only describes the algorithm of watermark embedding as bellow.

Step 1: Use (1) on cover image I to transform the RGB color space into the YCbCr color space to obtain I_Y, I_{Cb}, and I_{Cr} images. Let I be the image of size $m \times n$.

$$\begin{aligned} Y &= (0.257 \times R) + (0.504 \times G) + (0.098 \times B) + 16 \\ Cb &= -(0.148 \times R) - (0.291 \times G) + (0.439 \times B) + 128 \\ Cr &= (0.439 \times R) - (0.368 \times G) - (0.071 \times B) + 128 \end{aligned} \tag{1}$$

Step 2: Apply the one-level DWT to gray-level image I_Y to obtain four subband images $I_{Y,LL}$, $I_{Y,LH}$, $I_{Y,HL}$, and $I_{Y,HH}$. These subband images all are the image of size $(m/2) \times (n/2)$.

Step 3: Apply the DCT to the LL subband image $I_{Y,LL}$ to obtain frequency components D_Y. D_Y is the matrix of size $(m/2) \times (n/2)$.

Step 4: Apply SVD to frequency components D_Y to obtain matrix S_1, where the watermark image with the matrix of size $r \times r$, U_1 is a $(m/2) \times r$ matrix, S_1 is a $r \times r$ matrix with nonnegative numbers on the diagonal and zeros on the off diagonal, and V_1^T denotes the conjugate transpose of V_1, a $r \times (n/2)$ matrix. In this algorithm, $r = \min(m/2, n/2)$ was set.

$$D_Y = U_1 S_1 {V_1}^T \tag{2}$$

Step 5: Modify the singular values of S_1 with the watermark image W to obtain matrix S' as defined in (3), where β is the scale factor ($0 < \beta < 1$) which controls the strength of the watermark to be inserted, and S' is a $r \times r$ matrix. The scale factor is always defined and used in the known SVD-based image watermarking methods.

$$S' = S_1 + \beta W \tag{3}$$

Step 6: Apply SVD to matrix S' to obtain matrix S_2, where U_2 is a $(m/2) \times r$ matrix, S_2 is a $r \times r$ matrix with nonnegative numbers on the diagonal and zeros on the off diagonal, and V_2^T denotes the conjugate transpose of V_2, a $r \times (n/2)$ matrix.

$$S' = U_2 S_2 {V_2}^T \tag{4}$$

Step 7: Obtain watermarked image D_Y' by multiplying matrices U_1, S_2, and V_1^T, where D_Y' is a $(m/2) \times (n/2)$ matrix.

$$D_Y' = U_1 S_2 {V_1}^T \tag{5}$$

Step 8: Apply the inverse DCT to image D_Y' to obtain image $I_{Y,LL}'$. $I_{Y,LL}'$ is the image of size $(m/2) \times (n/2)$.

Step 9: Apply the inverse DWT to images $I_{Y,LL}'$, $I_{Y,LH}$, $I_{Y,HL}$, and $I_{Y,HH}$ to obtain image I_Y'. I_Y' is the image of size $m \times n$.

Step 10: Use (6) on image I_Y' with I_{Cb} and I_{Cr} to transform the YCbCr color space into the RGB color space, and then produce color watermarked cover image I_W. I_W is the image of size $m \times n$.

$$\begin{aligned} R &= 1.164(Y-16) + 1.596(Cr-128) \\ G &= 1.164(Y-16) - 0.391(Cb-128) - 0.813(Cr-128) \\ B &= 1.164(Y-16) + 2.018(Cb-128) \end{aligned} \tag{6}$$

2.2 Image matting

Automatic image matting using component-hue-difference-based spectral matting [11] is used to obtain the foreground object with the alpha matte. In component-hue-difference-based

spectral matting, adaptive component detection is first used to automatically obtain the distinct components of a given image. The mean shift [4] is used to obtain the clustering number, and then spectral segmentation with the k-means algorithm [25] using the obtained clustering number is applied to obtain the distinct components of the given image.

Once the number of clusters of a given image is obtained, it is applied to the spectral segmentation with the k-means algorithm based on the eigenvectors of the matting Laplacian matrix [17] to estimate the distinct components of a given image.

In image matting, it is typically assumed that each pixel I_i in an input image is a linear combination of a foreground color F_i and a background color B_i, as defined in (7), where α_i is the pixel's foreground opacity.

$$I_i = \alpha_i F_i + (1-\alpha_i) B_i \tag{7}$$

In spectral matting [18], the compositing equation is generalized by assuming that each pixel is a convex combination of K image layers $F^1 \sim F^K$, as defined in (8), where α_i^k are the matting components of a given image which specify the fractional contribution of each layer to the final color observed at each pixel and must satisfy (9). Furthermore, the given image consists of K distinct components $C_1 \sim C_K$ such that $C_i \cap C_j = \varphi$ for $i \neq j$.

$$I_i = \sum_{k=1}^{K} \alpha_i^k F_i^k \tag{8}$$

$$\sum_{k=1}^{K} \alpha_i^k = 1 \; ; \;\; \alpha_i^k \in [0,\ 1] \tag{9}$$

The average hue of each distinct component is then calculated in the HSV color space. If all hue angles between components are smaller than $\pi/5$, then a single foreground component and a single background component are found; otherwise, multiple foreground and background components are found.

The single foreground and background components are respectively obtained using (10) and (11), where $C(i)$ is the ith component; I_{boundary} is an image with boundary pixels (with a width of one pixel) of the given image; $C^H(i)$ is the hue angle of the ith component; and C_B and C_F are the background component and foreground component, respectively.

$$C_B = \arg\max_{i \in k} \left\{ C(i) \cap I_{\text{boundary}} \right\} \tag{10}$$

$$C_F = \arg\max_{i \in k} \left\{ C_B^H - C^H(i) \right\} \tag{11}$$

For the case of multiple foreground and background components, the adjacent components are first merged using the component merging algorithm. Next, the background component and foreground component are found using (10) and (11), respectively. Then, the foreground component and non-adjacent components are tested for further merging using the component merging algorithm. The background component is processed using the same procedure. Finally, the foreground, background, and unknown components are obtained.

The corresponding matting foreground, background, and unknown components are obtained using a linear transformation of the smallest eigenvectors of the matting Laplacian matrix [17]. The matting components are computed by minimizing an energy function, as defined in

(12), subject to $\sum_k \alpha_i^k = 1$ to find a set of $\widetilde{K}$ linear combination vectors y^k. The above energy function is optimally minimized using Newton's method.

$$\sum_{i,\,k} \left|\alpha_i^k\right|^{\gamma} + \left|1-\alpha_i^k\right|^{\gamma}, \quad \text{where } \alpha^k = \widetilde{E} y^k \tag{12}$$

Finally, the matting foreground and unknown components are combined to form the complete alpha matte by minimizing the matte cost:

$$J(\alpha) = \alpha^T L \alpha \tag{13}$$

The matting Laplacian matrix L is defined as a sum of matrices $L = \sum_q A_q$, each of which contains the affinities among pixels inside a local window w_q, where δ_{ij} is the Kronecker delta; μ_q is a 3×1 mean color vector in the window w_q around pixel q; $\sum_q$ is a 3×3 covariance matrix in a given window; $|w_q|$ is the number of pixels in a given window; $I_{3\times3}$ is the 3×3 identity matrix; I_i and I_j are 3×1 color vectors in the window w_q; and ε is a small positive constant.

$$A_q(i,j) = \begin{cases} \delta_{ij} - \dfrac{1}{|w_q|}\left(1 + \left(I_i - \mu_q\right)^T \left(\sum_q + \dfrac{\varepsilon}{|w_q|} I_{3\times3}\right)^{-1} \left(I_j - \mu_q\right)\right), & (i,j) \in w_q \\ 0, & \text{otherwise} \end{cases} \tag{14}$$

To perform this task efficiently, the correlations between the matting components via L are pre-computed and stored in a $\widetilde{K} \times \widetilde{K}$ matrix Φ, as defined in (15), and the matting cost can be computed using (16), where b is a $\widetilde{K}$ -dimensional binary vector indicating the selected matting components [18].

$$\Phi(k,l) = \alpha^{k^T} L \alpha^l \tag{15}$$

$$J(\alpha) = b^T \Phi b \tag{16}$$

Figure 2 shows the obtained result of image matting for the case of single foreground and background components. Figure 3 shows the obtained result of image matting for the case of multiple foreground and background components. In Figs. 2(c) and 3(c), the selected background component is green, the unknown components are blue, and the selected foreground component is the remaining region.

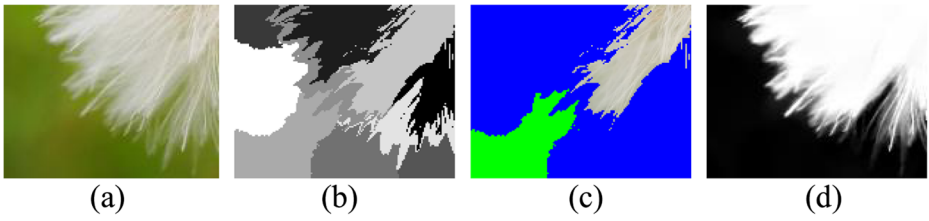

Fig. 2 Image matting of an image of a flower. **a** Original image, **b** result of component detection, **c** result of component classification, and (**d**) obtained alpha matte [11]

Fig. 3 Image matting of an image of Amira. **a** Original image, **b** result of component detection, **c** result of component classification, and (**d**) obtained alpha matte [11]

2.3 Proposed image forgery detection scheme

The proposed image forgery detection scheme has two parts; one is watermark embedding and the other is the identification of tampered images. A flow diagram of watermark embedding in the proposed image forgery detection scheme is shown in Fig. 4.

The algorithm of watermark embedding in the proposed image forgery detection scheme is described below.

Step 1: Use component-hue-difference-based spectral matting to obtain the alpha matte I_α of the cover image I.
Step 2: Use the obtained alpha matte I_α to extract the foreground and background images.
Step 3: Use the DWT-DCT-SVD-based watermarking method to embed two different watermarks into the foreground and background images to obtain the singular value

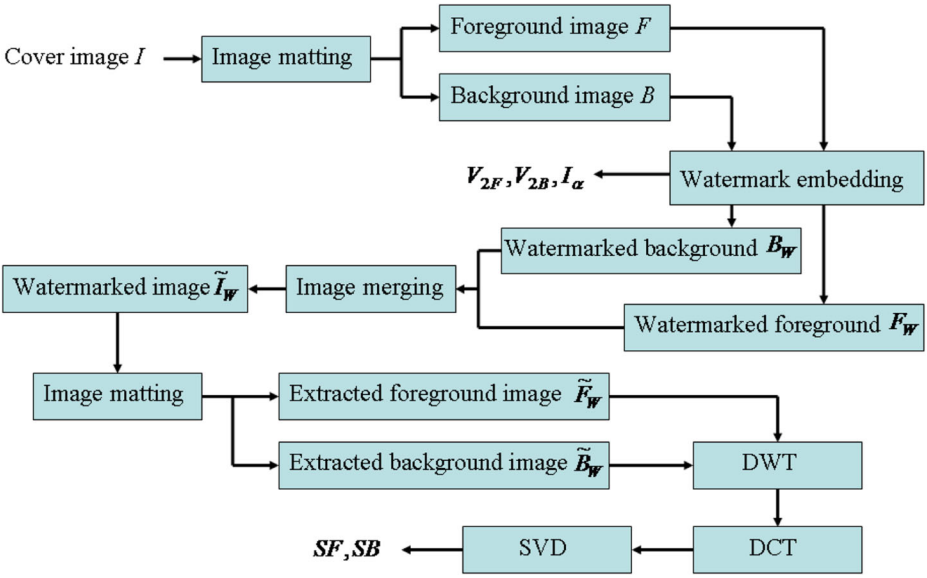

Fig. 4 Flow diagram of watermark embedding in the proposed image forgery detection scheme

matrices S_{2F} and S_{2B}, respectively. Let the singular value vectors of S_{2F} and S_{2B} be $V_{2F}=(\lambda_{2F}^0,\lambda_{2F}^1,....,\lambda_{2F}^{N-1})$ and $V_{2B}=(\lambda_{2B}^0,\lambda_{2B}^1,....,\lambda_{2B}^{N-1})$, respectively.

Step 4: Merge the watermarked foreground image F_W and watermarked background image B_W to obtain the watermarked cover image $\tilde{I}_W$.

Step 5: Use the obtained alpha matte I_α on the image $\tilde{I}_W$ to extract the foreground image $\widetilde{F}_W$ and background image $\widetilde{B}_W$.

Step 6: Transform images $\widetilde{F}_W$ and $\widetilde{B}_W$ from the RGB color space to the YCbCr color space using (1), and then obtain gray-level images $\widetilde{F}_{YW}$ and $\widetilde{B}_{YW}$, respectively.

Step 7: Apply the one-level DWT to images $\widetilde{F}_{YW}$ and $\widetilde{B}_{YW}$ to obtain $\widetilde{F}_{YW,LL}$ and $\widetilde{B}_{YW,LL}$, respectively.

Step 8: Apply the DCT to images $\widetilde{F}_{YW,LL}$ and $\widetilde{B}_{YW,LL}$ to obtain frequency components $D_{\widetilde{F}}$ and $D_{\widetilde{B}}$, respectively.

Step 9: Apply SVD to frequency components $D\widetilde{F}$ and $D\widetilde{B}$ to obtain singular value matrices $S_{W1\widetilde{F}}$ and $S_{W1\widetilde{B}}$, respectively. Let the singular value vectors of $S_{W1\widetilde{F}}$ and $S_{W1\widetilde{B}}$ be $V_{W1\widetilde{F}}=\left(\lambda_{W1\widetilde{F}}^0,\lambda_{W1\widetilde{F}}^1,....,\lambda_{W1\widetilde{F}}^{N-1}\right)$ and $V_{W1\widetilde{B}}=\left(\lambda_{W1\widetilde{B}}^0,\lambda_{W1\widetilde{B}}^1,....,\lambda_{W1\widetilde{B}}^{N-1}\right)$, respectively.

Step 10: Calculate *SF* and *SB* as the thresholds needed for identification of tampered images.

$$SF=\frac{1}{N}\sum_{i=0}^{N-1}\left|\lambda_{W1\widetilde{F}}^{i}-\lambda_{2F}^{i}\right| \tag{17}$$

$$SB=\frac{1}{N}\sum_{i=0}^{N-1}\left|\lambda_{W1\widetilde{B}}^{i}-\lambda_{2B}^{i}\right| \tag{18}$$

Step 11: Output V_{2B}, V_{2F}, *SB*, *SF*, and alpha matte I_α.

In the watermark embedding algorithm of the proposed image forgery detection scheme, the foreground image is obtained using the composition of a base map in black and the foreground part obtained using the cover image with the alpha matte. The background image is obtained using the composition of a base map in black and the background part obtained using the cover image with the alpha matte. However, there are slight changes in the singular values of the obtained watermarked foreground and background images after the merging scheme is applied. Therefore, steps 5–10 in the watermark embedding algorithm are used to obtain the difference between the singular values as the thresholds needed for the identification of tampered images.

Figure 5 shows a flow diagram of the identification of tampered images in the proposed image forgery detection scheme. The algorithm for identifying tampered images is described below.

Input: V_{2B}, V_{2F}, *SB*, *SF*, and alpha matte of tested image I_α.

Step 1: Use the obtained alpha matte I_α on the cover image I_W to extract the foreground and background images, and then further transform them from the RGB color space to the YCbCr color space using (1) to obtain the gray-level images F_{YW} and B_{YW}, respectively.

Step 2: Apply the one-level DWT to images F_{YW} and B_{YW} to obtain $F_{YW,LL}$ and $B_{YW,LL}$, respectively.

Step 3: Apply the DCT to images $F_{YW,LL}$ and $B_{YW,LL}$ to obtain frequency components D_F and D_B, respectively.

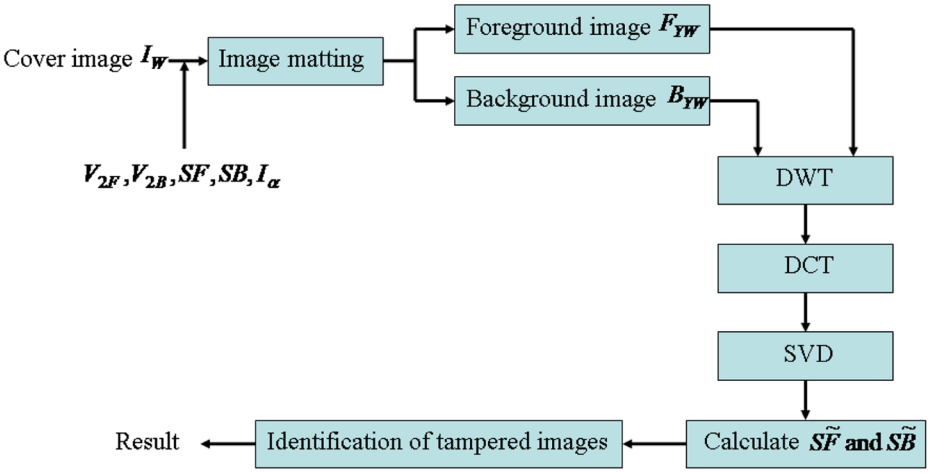

Fig. 5 Flow diagram of the proposed image forgery detection

Step 4: Apply SVD to frequency components D_F and D_B to obtain singular value matrices S_{W1F} and S_{W1B}, respectively. Let the singular value vectors of S_{W1F} and S_{W1B} be $V_{W1F} = \left(\lambda^0_{W1F}, \lambda^1_{W1F}, ..., \lambda^{N-1}_{W1F}\right)$ and $V_{W1B} = \left(\lambda^0_{W1B}, \lambda^1_{W1B}, ..., \lambda^{N-1}_{W1B}\right)$, respectively.

Step 5: Calculate $S\widetilde{F}$ and $S\widetilde{B}$.

$$S\widetilde{F} = \frac{1}{N}\sum_{i=0}^{N-1}\left|\lambda^i_{W1F} - \lambda^i_{2F}\right| \tag{19}$$

$$S\widetilde{B} = \frac{1}{N}\sum_{i=0}^{N-1}\left|\lambda^i_{W1B} - \lambda^i_{2B}\right| \tag{20}$$

Step 6: Identification of tampered images is obtained using the following rules, where Th_F and Th_B are the thresholds used to mainly check the forged foreground and forged background, respectively, and Th'_F and Th'_B are the thresholds used to mainly check the exchanged foreground and exchanged background, respectively.

$$Foreground\ Event = \begin{cases} It\ is\ forged & ,If\ SF_D > Th_F \& SF_D \le Th'_F \\ It\ is\ exchanged & ,If\ SF_D > Th_F \& SF_D > Th'_F \& SB_D > Th_B \\ It\ is\ neither\ forged\ nor\ exchanged & ,otherwise \end{cases} \tag{21}$$

$$Background\ Event = \begin{cases} It\ is\ forged & ,If\ SB_D > Th_B \& SB_D \le Th'_B \\ It\ is\ exchanged & ,If\ SB_D > Th_B \& SB_D > Th'_B \& SF_D > Th_F \\ It\ is\ neither\ forged\ nor\ exchanged & ,otherwise \end{cases} \tag{22}$$

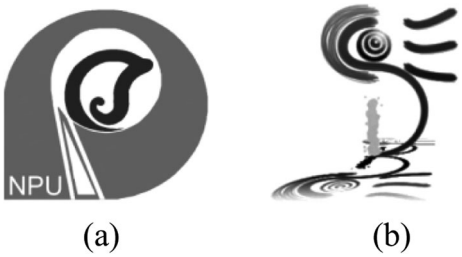

Fig. 6 Watermarks. **a** NPU-logo (watermark for foreground image) and (**b**) CSIE-logo (watermark for background image)

$$SF_D = S\widetilde{F}/SF \tag{23}$$

$$SB_D = S\widetilde{B}/SB \tag{24}$$

$$Th_F = 1 + \frac{1}{N_1}\sum_{i=1}^{N_1}\alpha_i\ ,\ \forall\alpha_i > 0 \tag{25}$$

$$Th_B = 1 + \frac{1}{N_2}\sum_{i=1}^{N_2}(1-\alpha_i)\ ,\ \forall\alpha_i < 1 \tag{26}$$

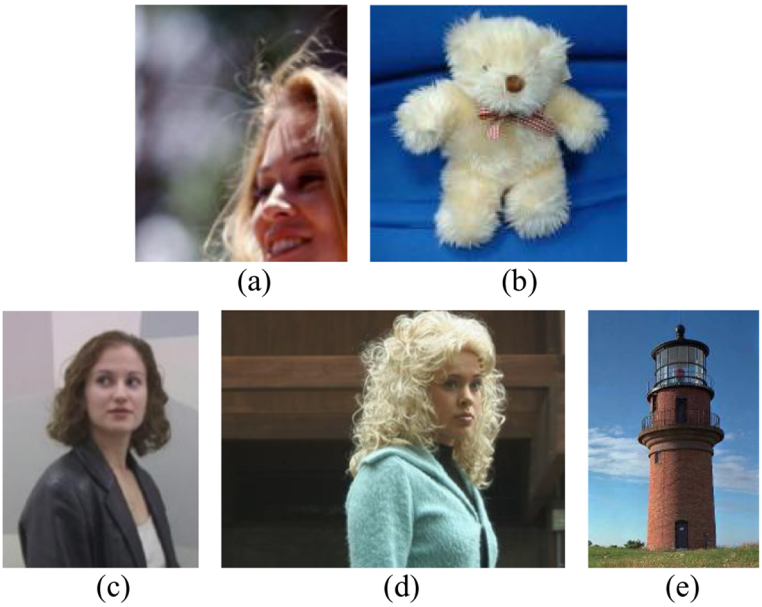

Fig. 7 Tested images. **a** Face, **b** Bear, **c** Amira, **d** Kim, and (**e**) Pharos

$$Th_F^{'} = 2{\cdot}SF/\left(\frac{1}{N_1}\sum_{i=1}^{N_1}\alpha_i\right)^2,\ \forall\alpha_i > 0 \tag{27}$$

$$Th_B^{'} = 2{\cdot}SB/\left(\frac{1}{N_2}\sum_{i=1}^{N_2}(1-\alpha_i)\right)^2,\ \forall\alpha_i < 1 \tag{28}$$

Step 7: Output the result of tampered image identification.

It is worth mentioning that the SVD-based image watermarking has the false positive detection of watermarks [23, 26, 28]. Although DWT-DCT-SVD-based image watermarking is used in the proposed image forgery detection scheme, false-positive detection is not considered in the proposed method because the watermark image does not need to be extracted using its matrices U and V to detect tampered images. Only the singular value vectors are used to identify tamped images.

Furthermore, the thresholds used in (21) and (22) are not given by users. They are adaptive values based on tested images. Therefore, the proposed image forgery detection scheme is suitable for practical applications.

3 Experimental results

Experiments were conducted on a computer with an Intel Core i5-2400 3.1-GHz CPU and 8GB of RAM. The algorithms were implemented in Matlab R2011a. NPU-logo and CSIE-

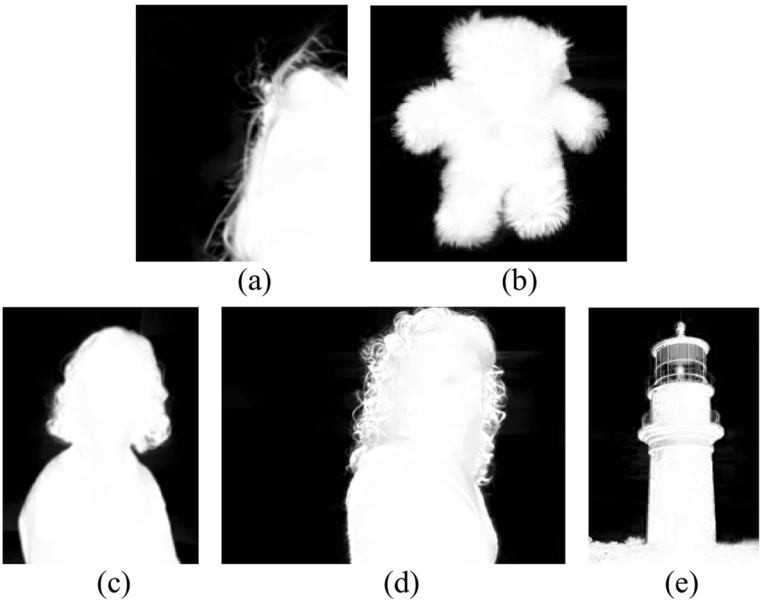

Fig. 8 Alpha mattes of (**a**) Face, **b** Bear, **c** Amira, **d** Kim, and (**e**) Pharos

logo were used to watermark the foreground and background images, respectively, as shown in Fig. 6(a) and (b).

Five images were used as authentic images of image forgery detection. Figure 7(a–e) show images of the images Face, Bear, Amira, Kim, and Pharos, respectively, and Fig. 8(a–e) show their corresponding alpha mattes, respectively. Each authentic image was undergone some form of manipulation or alteration, which included exchanged background image with 15 different images, exchanged foreground image with 15 different images, tampered foreground image with 15 different ways, tampered background image with 15 different ways, and both tampered foreground image and tampered background image with 4 different ways. Therefore, a self-made dataset that includes 320 images saved with double JPEG compression was used to evaluate the performance of image forgery detection.

Figures 9, 10, 11, 12, and 13 are the results obtained using the proposed image forgery detection scheme, and they are some samples in the image dataset. Figures 9(a, b, c and d), 10(a, b, c and d), 11(a, b, c and d), 12(a, b, c and d) and 13(a, b, c and d) are the detected results of an exchanged background image, an exchanged foreground image, a tampered foreground image, and a tampered background image, respectively.

Figures 9(a), 10(a), 11(a), 12(a) and 13(a) are composite images created by composing the foreground images and new background images using the alpha mattes. Figures 9(b), 10(b), 11(b), 12(b) and 13(b) are composite images created by composing the background images and new foreground images using the alpha mattes. Experimental results show that the proposed method

Fig. 9 Image forgery detection of Face. Detection results for (**a**) exchanged background image, **b** exchanged foreground image, **c** tampered foreground image, and (**d**) tampered background image

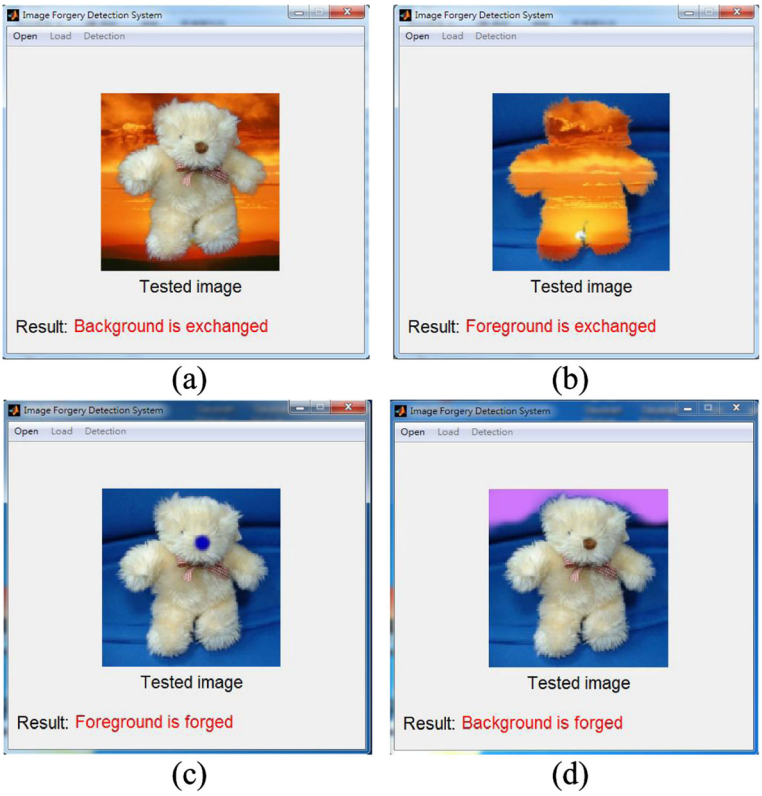

Fig. 10 Image forgery detection of Bear. Detection results for (**a**) exchanged background image, **b** exchanged foreground image, **c** tampered foreground image, and (**d**) tampered background image

can accurately and effectively detect image forgery for exchanged foreground or background images.

In Fig. 9(c), the color of the girl's eyebrows has been changed. Therefore, the proposed image forgery detection scheme reports that the foreground is forged. In Fig. 9(d), one region of the background image has been copied and moved to another background part. Therefore, the proposed image forgery detection scheme reports that the background is forged.

In Fig. 10(c), the color of the bear's nose has been changed. Therefore, the proposed image forgery detection scheme reports that the foreground is forged. In Fig. 10(d), the color of the upper region in the background image has been changed. Therefore, the proposed image forgery detection scheme reports that the background is forged.

In Fig. 11(c), one region of Amira's clothes has been copied and moved to another foreground part. Therefore, the proposed image forgery detection scheme reports that the foreground is forged. In Fig. 11(d), one region of the background image has been copied and moved to another background part. Therefore, the proposed image forgery detection scheme reports that the background is forged.

In Fig. 12(c), the color of Kim's sweater has been changed. Therefore, the proposed image forgery detection scheme reports that the foreground is forged. In Fig. 12(d), one region of the foreground image has been copied and moved to the background part. Therefore, the proposed image forgery detection scheme reports that the background is forged.

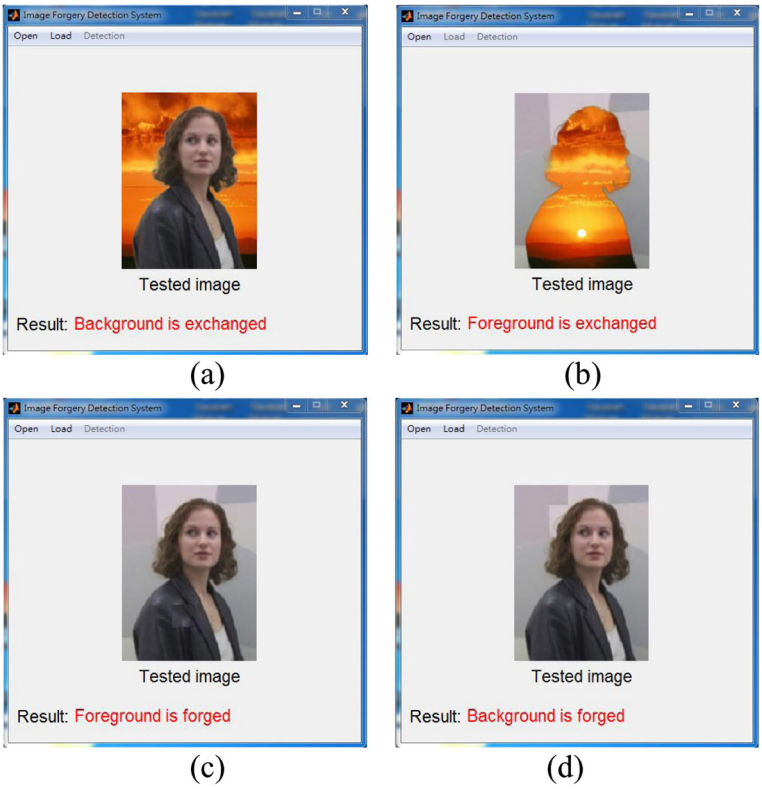

Fig. 11 Image forgery detection of Amira. Detection results for (**a**) exchanged background image, **b** exchanged foreground image, **c** tampered foreground image, and (**d**) tampered background image

In Fig. 13(c), the lighthouse door has been covered by one region of the foreground image. Therefore, the proposed image forgery detection scheme reports that the foreground is forged. In Fig. 13(d), the left-corner region of the background image has been scribbled on. Therefore, the proposed image forgery detection reports that the background is forged.

Four state-of-the-art method, the image watermarking method proposed by Lai and Tsai [16], the copy-move forgery detection proposed by Huang et al. [13], the tampering detection of composite images proposed by Lin et al. [21], and the image forgery detection proposed by Hu et al. [9], were used to compare with the proposed method to evaluate the performance in the self-made dataset. In the image watermarking method proposed by Lai and Tsai [16], the identification of tampered images needs to give threshold by users based on peak signal-to-noise ratio (PSNR) and correlation coefficient (CC) in this experiment because the identification rule was not given in the literature.

In order to illustrate the performance of image forgery detection, the detection accuracy D_a was adopted as defined in Eq. (29), where P is the total number of images, and TP is the total number of true positive images. Table 1 shows the results of the performance evaluation for the self-made dataset, where algorithm 1 is the image watermarking method proposed by Lai and Tsai [16], algorithm 2 is the copy-move forgery detection proposed by Huang et al. [13], algorithm 3 is the tampering detection of composite images proposed by Lin et al. [21], algorithm 4 is the image forgery detection proposed by Hu et al. [9], and algorithm 5 is the proposed method. Experimental results show that the proposed method outperforms state-of-

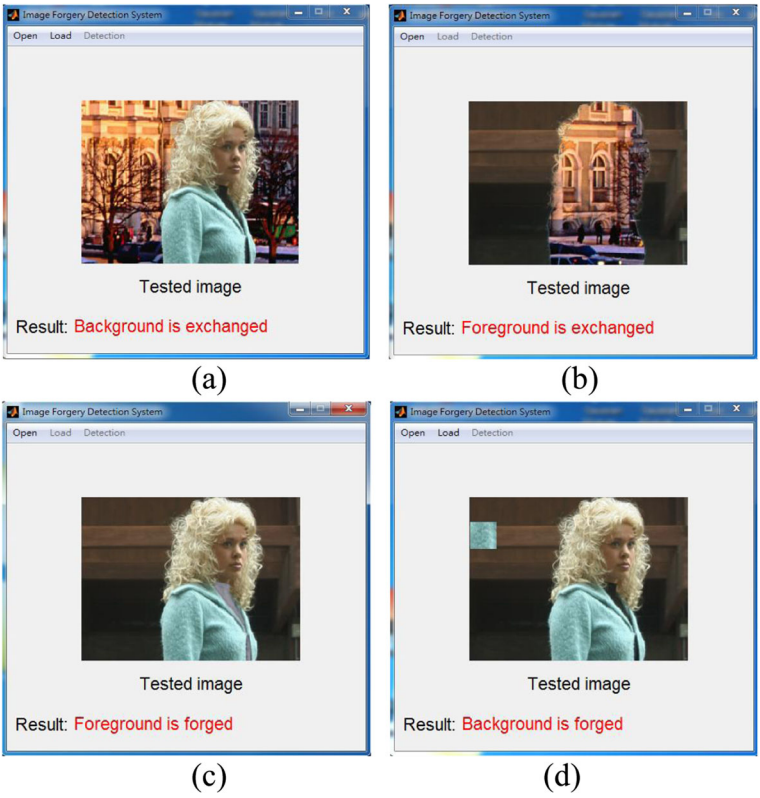

Fig. 12 Image forgery detection of Kim. Detection results for (**a**) exchanged background image, **b** exchanged foreground image, **c** tampered foreground image, and (**d**) tampered background image

the-art methods [9, 13, 16, 21] for image forgery detection.

$$D_a = \left(\frac{TP}{P}\right) \times 100\% \tag{29}$$

The reasons of low detection accuracy using the image watermarking method proposed by Lai and Tsai [16] have two: (1) The area of changed region (tampered region) is too small; and (2) The given identification rule may be not optimal.

The reason of low detection accuracy using the copy-move forgery detection proposed by Huang et al. [13] is that this method only works well for the forgery image created by copying and pasting regions from the same image.

The reasons of low detection accuracy using the tampering detection of composite images proposed by Lin et al. [21] have two: (1) The quality of second JPEG compression is not higher than that of the original JPEG of the unchanged region; and (2) The area of changed region (tampered region) is not moderate (changed region should be within 30–70 % of the image).

The reason of low detection accuracy using the image forgery detection proposed by Hu et al. [9] is that this method only works well for forgery images with exchanged foreground image or exchanged background image.

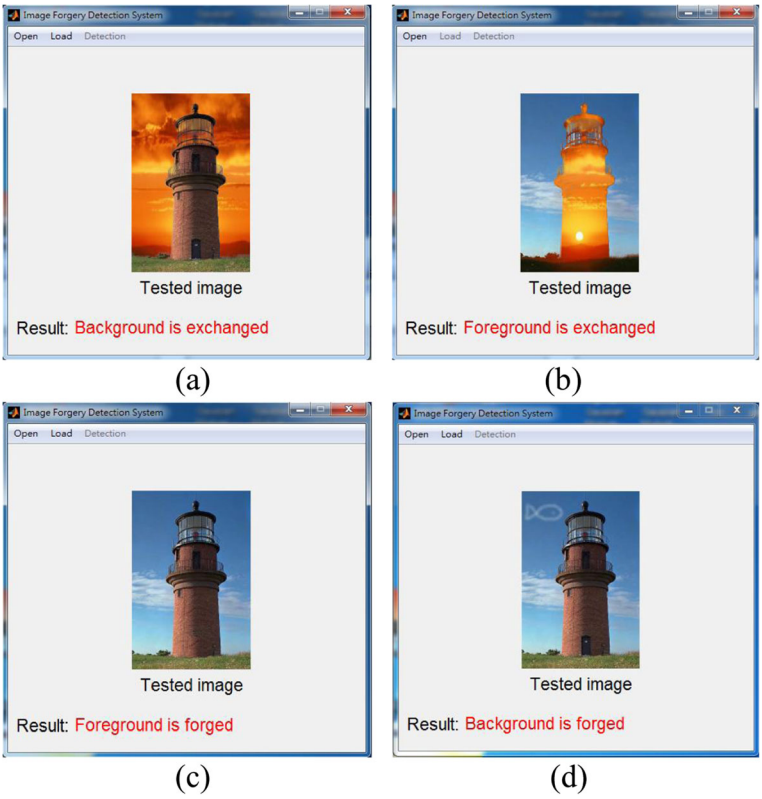

Fig. 13 Image forgery detection of Pharos. Detection results for (**a**) exchanged background image, **b** exchanged foreground image, **c** tampered foreground image, and (**d**) tampered background image

The proposed method may make tampering detection fail for forgery images with both tampered foreground image and tampered background image. Experimental results show that the proposed method can accurately and effectively detect tampered foreground or background images. Furthermore, the proposed method can accurately detect a tampered region that is only about 1 % of the tested image.

The difference between the proposed method and the previous work [9] is described below. (1) In the previous work, the identification of tampered images is used the given threshold by users, and thus the previous work can not work well for practical applications. Compared with the previous work, the proposed method uses adaptive thresholds to obtain identification of tampered images, and thus the proposed method can work well for practical applications. (2) The previous work only works well for identifying exchanged foreground images or exchanged background images. Compared with the

Table 1 Performance evaluation for a self-made dataset

	Algorithm 1 [16]	Algorithm 2 [13]	Algorithm 3 [21]	Algorithm 4 [9]	Algorithm 5
TP	286	105	218	150	310
D_a	89.38 %	32.81 %	68.13 %	46.88 %	96.88 %

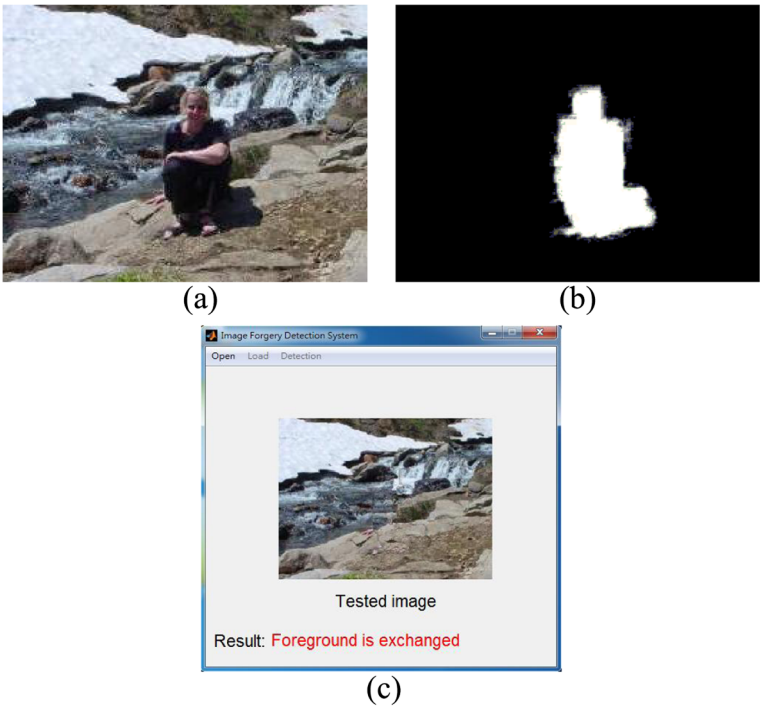

Fig. 14 Image forgery detection of image conducted using exemplar-based inpainting. **a** Original image, **b** alpha matte, and (**c**) detection result of exchanged foreground image

previous work, the proposed method works well for identifying exchanged foreground images, exchanged background images, tampered foreground images, or tampered background images.

It is worth mentioning that component-hue-difference-based spectral matting [11] used in the proposed image forgery detection scheme can be replaced by other image matting methods (such as easy matting [6] and closed-form matting [17]) to improve image forgery detection. Furthermore, DWT-DCT-SVD-based image watermarking [10] used in the proposed image forgery detection scheme can also be replaced by other SVD-based image watermarking schemes (such as DWT-SVD-based scheme [16] and SVD-GA-based scheme [15]).

Furthermore, for the obtained results of tampered foreground image or tampered background image using the proposed method, the known passive forensic approaches (such as

Table 2 Computational cost using the proposed method for forgery images

Category of forgery image	Size of forgery image	Computational cost (ms)
Face	140×170	27.38
Bear	150×150	19.93
Amira	160×210	29.33
Kim	318×238	52.12
Pharos	160×240	30.98

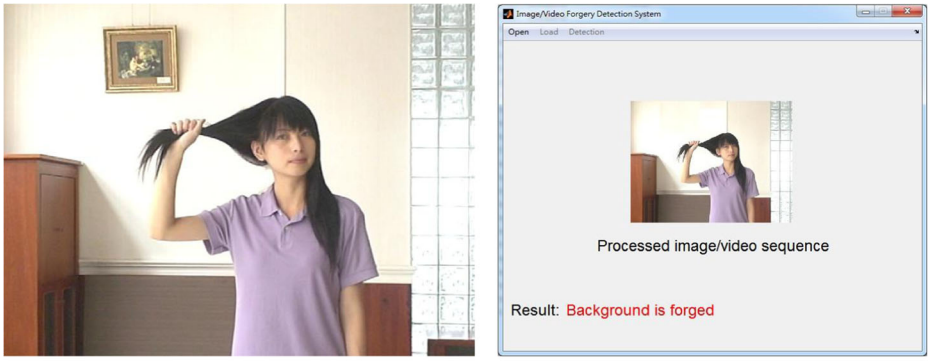

Fig. 15 Image forgery detection of Lobby. **a** Original image and (**b**) detection result of tampered background image

copy-move forgery detection [3, 14, 19] or tampering detection of composite images [1, 20, 24]) can be used to obtain the tampered regions of forged images. The accuracy can be effectively increased because only the foreground part or background part needs to check to obtain the tampered regions.

Figure 14 shows an example of image forgery conducted using exemplar-based image inpainting [5]. The alpha matte was obtained using closed-form matting [17], as shown in Fig. 14(b). The proposed method accurately detects the exchanged foreground image. This example only demonstrated that the proposed method can be used for the foreground image tampered using exemplar-based image inpainting [5]. Results tampered using other image inpainting schemes maybe don't be detected using the proposed method. The forgery detection algorithm proposed by Chang et al. [2] can work well for inpainting forged images. But, this approach only can work for the forgery image created by copying and pasting regions from the same image.

The algorithm of watermark embedding in the proposed method is off-line worked, and only image forgery detection in the proposed method is on-line worked. Let the tampered image be the image of size $m \times n$ and $N = m \times n$. The time complexity of DWT, DCT, and SVD in image forgery detection of the proposed method are $O(N)$, $O(N)$, and $O(r^3)$, respectively, where $r = \min(m/2, n/2)$ and the watermarking image with size $r \times r$. Therefore, the time complexity of the proposed method is $O(r^3)$. The computational cost using the proposed method is listed in Table 2. Figure 15 shows an example of forgery image with size 640×480, and the computational cost is 183.92 ms. Therefore, the computation cost using the proposed method to detect the forgery image is suitable and acceptable.

4 Conclusion

An image forgery detection scheme was proposed to effectively identify a tampered foreground or background image using image watermarking and alpha mattes. The component-hue-difference-based spectral matting [11] is first used to obtain the alpha matte. Next, DWT-DCT-SVD-based image watermarking [10] is used to embed the watermarks. Two different watermarks are embedded into the foreground and background images, respectively, based on obtained alpha mattes. Finally, the difference

between the obtained singular values is used to detect tampered foreground and background images.

The proposed method can accurately detect exchanged foreground images, exchanged background images, tampered foreground images, and tampered background images, and can detect forgery images created using image matting or image inpainting. Furthermore, the proposed method uses adaptive thresholds, making it suitable for practical applications. Moreover, the false-positive detection in SVD-based image watermarking does not affect the results obtained using the proposed method because only the singular value vectors are used to detect tampered images. Experimental results show that the proposed method has good performance on image forgery detection.

Acknowledgment This paper has been supported by the National Science Council, Taiwan, under grant no. NSC102-2221-E-346-007. The authors wish to express the appreciation to Prof. Chih-Chin Lai and Prof. Zhouchen Lin for their help with the experiments. The authors also gratefully acknowledge the helpful comments and suggestions of reviewers, which have improved the quality and presentation.

References

1. Bianchi T, Piva A (2012) Image forgery localization via block-grained analysis of JPEG artifacts. IEEE Trans Inf Forensic Secur 7(3):1003–1017
2. Chang I-C, Yu JC, Chang C-C (2013) A forgery detection algorithm for exemplar-based inpainting images using multi-region relation. Image Vis Comput 31(1):57–71
3. Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E (2012) An evaluation of popular copy-move forgery detection approaches. IEEE Trans Inf Forensic Secur 7(6):1841–1854
4. Comaniciu D, Meer P (2002) Mean shift: a robust approach toward feature space analysis. IEEE Trans Pattern Anal Mach Intell 24(5):603–619
5. Criminisi A, Perez P, Toyama K (2004) Region filling and object removal by exemplar-based image inpainting. IEEE Trans Image Process 13(9):1200–1212
6. Guan Y, Chen W, Liang X, Ding Z, Peng Q (2008) Easy matting: a stroke based approach for continuous image matting. Comput Graph Forum 25(3):567–576
7. Han Q, Han L, Wang E, Yang J (2013) Dual watermarking for image tamper detection and self-recovery. In: Proc. of the 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 33–36
8. Hu W-C, Chen W-H (2013) Effective forgery detection using DCT + SVD-based watermarking for region of interest in key frames of vision-based surveillance. Int J Comput Sci Eng 8(4):297–305
9. Hu W-C, Chen W-H, Huang D-Y, Yang C-Y (2012) Novel detection of image forgery for exchanged foreground and background using image watermarking based on alpha matte. In: Proc. of the 6th International Conference on Genetic and Evolutionary Computing, pp. 245–248
10. Hu W-C, Chen W-H, Yang C-Y (2012) Robust image watermarking based on discrete wavelet transform-discrete cosine transform-singular value decomposition. J Electron Imaging 21(3):033005(1)–033005(7)
11. Hu W-C, Hsu J-F (2013) Automatic spectral video matting. Pattern Recogn 46(4):1183–1194
12. Hu W-C, Jhu J-J, Lin C-P (2012) Unsupervised and reliable image matting based on modified spectral matting. J Vis Commun Image Represent 23(4):665–676
13. Huang D-Y, Lin T-W, Hu W-C, Chou C-H (2013) Boosting scheme for detecting region duplication forgery in digital images. In: Proc. of the 7th International Conference on Genetic and Evolutionary Computing, pp. 125–133
14. Huang Y, Lu W, Sun W, Long D (2011) Improved DCT based detection of copy-move forgery in images. Forensic Sci Int 206(1–3):178–184
15. Lai C-C (2011) A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. Digit Signal Process 21:522–527
16. Lai C-C, Tsai C-C (2010) Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans Instrum Meas 59:3060–3063
17. Levin A, Lischinski D, Weiss Y (2008) A closed-form solution to natural image matting. IEEE Trans Pattern Anal Mach Intell 30(2):228–242

18. Levin A, Rav-Acha A, Lischinski D (2008) Spectral matting. IEEE Trans Pattern Anal Mach Intell 30(10): 1699–1712
19. Li L, Li S, Zhu H, Chu S-C, Roddick JF, Pan J-S (2013) An efficient scheme for detecting copy-move forged images by local binary patterns. J Inf Hiding Multimedia Signal Process 4(1):46–56
20. Lin G-S, Chang M-K, Chen Y-L (2011) A passive-blind forgery detection scheme based on content-adaptive quantization table estimation. IEEE Trans Circ Syst Video Technol 21(4):421–434
21. Lin Z, He J, Tang X, Tang CK (2009) Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis. Pattern Recogn 42(11):2492–2501
22. Liu K-C (2012) Colour image watermarking for tamper proofing and pattern-based recovery. IET Image Process 6(5):445–454
23. Loukhaoukha K, Chouinard JY (2010) On the security of ownership watermarking of digital images based on SVD decomposition. J Electron Imaging 19(1):013007(1)–013007(9)
24. Mahdian B, Saic S (2009) Using noise inconsistencies for blind image forensics. Image Vis Comput 27(10): 1497–1503
25. Ng A, Jordan M, Weiss Y (2001) On spectral clustering: analysis and an algorithm. Adv Neural Inf Process Syst 14:849–856
26. Rykaczewski R (2007) Comments on An SVD-based watermarking scheme for protecting rightful ownership. IEEE Trans Multimedia 9(2):421–423
27. Wang J, Cohen MF (2007) Image and video matting: a survey. Found Trends Comput Graph Vis 3(2):1–78
28. Zhang X-P, Li K (2005) Comments on an SVD-based watermarking scheme for protecting rightful ownership. IEEE Trans Multimedia 7(2):593–594

Wu-Chih Hu received his Ph.D. degree in electrical engineering from the National Taiwan University of Science and Technology, Taipei, Taiwan, in 1998. From 1998, he worked at the National Penghu University of Science and Technology for 16 years. He is currently the chairman and Professor in the Department of Computer Science and Information Engineering. He has published more than 100 papers in journal and conference proceedings since 1998. He obtained the Best Paper Awards of ICGEC2010, RVSP2011, ACIIDS2012, ISIC2012, and ICGEC2013. His current research interests include computer vision, image processing, pattern recognition, digital watermarking, visual surveillance, and video processing.

Wei-Hao Chen received his MS degree in Graduate Institute of Electrical Engineering and Computer Science, National Penghu University of Science and Technology, Taiwan, in 2012. His recent research interests include image processing and digital watermarking.

Deng-Yuan Huang received his Ph.D. degree in Aeronautic and Astronautic Engineering from National Cheng Kung University, Taiwan, in 1994. He was with the steel and alumina R&D department at CSC Inc. for several years as an associate scientist specializing in process control in steel-making. He joined the Department of Electrical Engineering at Dayeh University in 2002 and is currently an associate professor. He obtained the Best Paper Awards of ICGEC2010, RVSP2011, ISIC2012, and ICGEC2013. He has published over 70 papers in journals and conference proceedings since 2002. His major research interests include image processing, pattern recognition, and computer vision.

Ching-Yu Yang received his B.S. degree in electronic engineering in 1983 from National Taiwan Institute of Technology and M.S. degree in electrical engineering in 1990 from National Cheng Kung University, Taiwan. In 1999 he received his Ph.D. degree in Computer and Information Science from National Chiao Tung University. In 1999–2005, he was a senior engineer at Chunghwa Telecom. Co. Ltd., Taiwan. He joined the Computer Science and Information Engineering at National Penghu University of Technology in February 2005, and is currently an associate professor there. His recent research interests include image processing, data hiding and network security.