

Yan WO, Guoqiang HAN

# Image content authentication technique based on Laplacian Pyramid

© Higher Education Press and Springer-Verlag 2008

**Abstract** This paper proposes a technique of image content authentication based on the Laplacian Pyramid to verify the authenticity of image content. First, the image is decomposed into Laplacian Pyramid before the transformation. Next, the smooth and detail properties of the original image are analyzed according to the Laplacian Pyramid, and the properties are classified and encoded to get the corresponding characteristic values. Then, the signature derived from the encrypted characteristic values is embedded in the original image as a watermark. After the reception, the characteristic values of the received image are compared with the watermark drawn out from the image. The algorithm automatically identifies whether the content is tampered by means of morphologic filtration. The information of tampered location is presented at the same time. Experimental results show that the proposed authentication algorithm can effectively detect the event and location when the original image content is tampered. Moreover, it can tolerate some distortions produced by compression, filtration and noise degradation.

**Keywords** digital watermark, image authentication, Laplacian Pyramid, digital signature, morphology

## 1 Introduction

The goal of image authentication is to verify the integrity of an image to avoid tampering. Currently, image authentication schemes can be classified into two: entire authentication and content authentication [1,2]. Entire authentication schemes pay more attention to the integrity of data, and modifying image information is not allowed. Based on the digital signature technique in message authentication, Hash

function and cryptogram systems are applied to resist forgery in the entire authentication. For the properties of Hash function, since a small perturbation can distinctly change the function value, it is highly sensitive to image processes of preserving content such as compression, filtering and so on. The image disposed by these image processes will not pass through verification, although its content was not changed. The feature-based image content algorithms [3–5] generate an authentication sign by drawing out the image feature (for example, edge feature). When authenticating, according to the similarity of the feature, we can judge whether the image has been tampered. Then, according to the position of the variation feature, we can confirm the tampered location. The feature-based image content algorithms can verify the tampering efficiently, and it can tolerate some distortions produced by image compression and other processes that do not alter the content. Sometimes, tampering can imitate the original image by generating a forge image which has the same feature. For example, most feature-based image content algorithms select the edge feature to verify the image. However, two images may have the same edge feature with different colors.

Smooth component and edge feature are drawn out in Ref. [6] with dyadic wavelet transform multi-scale edge detection technique as the feature sets of image content authentication. This algorithm overcomes the shortcomings of content authentication-based edge feature. It can not only tolerate some compression damages, noise pollution and other image processions not affecting the image content, but can also effectively prevent image counterfeiting. However, it still has some deficiencies. First, it generates a summary of 128 bits with Hash function after smooth component quantification. For the sensitive feature of Hash function, two images can be considered as the same only when their smooth components are equal. Second, because misdetection may occur when extracting the watermark, the summary of smooth component cannot be embedded in the original image with the watermark, and it can only be appended to the image file as accessional information. This accessional information needs additional memory, and it is easy to be tampered or lost.

Translated from *Journal of South China University of Technology (Natural Science Edition)*, 2007, 35(1): 34–38 [译自: 华南理工大学学报 (自然科学版)]

Yan WO (✉), Guoqiang HAN  
School of Computer Science and Engineering, South China University of Technology, Guangzhou 510640, China  
E-mail: woyan@scut.edu.cn

To solve these problems, an image content authentication technique based on Laplacian Pyramid is proposed in this paper based on previous researches [6–8]. At first the image is decomposed into Laplacian Pyramid. Then at the sending end, the smooth and the detail properties of the original image are analyzed according to the Laplacian Pyramid and encoded to get the corresponding characteristic values. After encryption, the signature derived from the encrypted characteristic values will be embedded in the original image as a watermark. At the receiving end, the characteristic values derived from the image in the same way will be compared with the characteristic values drawn out from the watermark. To the difference image, it verifies automatically whether the image content is tampered and pinpoints the tampered location by means of morphologic filtration.

## 2 Laplacian Pyramid and image feature extraction

Edge feature is the most important information of an image, which has a significant function in human visual perception and object recognition. Hence, many researchers apply the edge feature to verify image content tampering [3–5]. However, this technique has a specific limitation. It is possible that there are two images of different contents which have identical edge maps. For example, if a red light in a traffic image was tampered to be a green light, it cannot be checked with feature-based image content authentication because only the points where the image intensity has sharp transitions are contained in the edge feature, while the feature of the smooth part is neglected. The edge feature cannot reflect the change of the smooth part of an image, yet the change is important in human visual perception. Therefore, when verifying image content, we should pay attention not only to the edge feature but also to the smooth part.

After Laplacian Pyramid transformation, an image sequence with degressive resolution is generated. On the top is an approximate of low resolution of the image that describes the basic content. The other layers describe the details of different resolution. In this paper, smooth and detailed properties of the image are investigated by Laplacian Pyramid transform, and the image content authentication is just according to the two properties.

### 2.1 Laplacian Pyramid

Laplacian Pyramid is derived from Gaussian pyramid decomposition. Let  $f$  be the original image, the Gaussian pyramid can be produced by Eq. (1):

$$\mathbf{G}_k = \begin{cases} f, & k=0 \\ \text{reduce}(\mathbf{G}_{k-1} * \theta), & 1 \leq k \leq N \end{cases} \quad (1)$$

The mark “\*” denotes convolution;  $\theta$  is Gaussian low-pass filter;  $N$  is the max level number of the Gaussian pyramid.  $\text{reduce}(\cdot)$  is reduce sub-sample operator. According to Eq. (1), to get the Gaussian pyramid, process the lower level by Gaussian low-pass filter, then sample it at an interval of lines and rows with  $\text{reduce}$  (2). The upper level is four times smaller than the lower level. The images ranging from low to high are Gaussian pyramid.

The Laplacian Pyramid is a sequence of error images  $L_0, L_1, \dots, L_N$ . Each is the difference between two levels of the Gaussian pyramid.

$$L_k = \begin{cases} \mathbf{G}_N, & k=N \\ \mathbf{G}_k - \text{expand}(\mathbf{G}_{k+1}), & 0 \leq k < N \end{cases} \quad (2)$$

Here,  $\text{expand}(\cdot)$  is the expand operator, i.e., over sample. An image can be reconstructed by the Laplacian Pyramid, so it can be represented with its Laplacian Pyramid.  $L_N$  is a coarse approximate of the image describing its smooth feature. It is used to analyze the image’s structure and integral content.  $L_1 - L_{N-1}$  denotes the detail signals on different resolutions. To verify whether the image has been tampered or not, we should consider not only the integral content but also the details. Image feature extraction includes smooth feature extraction and edge feature extraction in this paper.

### 2.2 Smooth properties extraction and coding

In the course of feature extraction, the image is divided into four levels of Laplacian Pyramid. The pixel  $S(i, j)$  of the feature image is represented by 3 bit, hereinto the top two bits  $S_3(i, j)$  and  $S_2(i, j)$  represent smooth properties, and the lowest bit  $S_1(i, j)$  represents detailed properties. The lowest resolution image  $L_4$  of Laplacian Pyramid representing the coarse proximate image is smooth properties. In view of the influence of noises, the top two bits are extracted as characteristic value code. Let  $L_4$  be constituted by  $P$  bit planes, i.e.,

$$L_4(i, j) = \sum_{k=0}^{P-1} x_k(i, j) 2^k, \quad x_k(i, j) \in \{0, 1\}. \quad (3)$$

Then, smooth properties are coded with two bits:

$$S_3(i, j) = x_{P-1}(i, j), \quad S_2(i, j) = x_{P-2}(i, j). \quad (4)$$

Original image  $f(x, y)$  will possibly be disposed by different processes such as compression, filtering or tampering in the process of transmission, storage, modification, and accessing. After these processes, we get the observed image  $g(x, y)$  and the difference  $\eta(x, y)$  between  $f(x, y)$  and  $g(x, y)$ . Their relationship is represented as follows:

$$g(x, y) = f(x, y) + \eta(x, y). \quad (5)$$

By Laplacian Pyramid, the lowest resolution image  $L_N^*$  is obtained from  $g(x, y)$ . Because of Eqs. (1) and (2),  $L_N$  and  $L_N^*$  can be considered as the result sampled from  $f(x, y)$  and  $g(x, y)$ , which are processed by Gaussian filter  $\theta$ . Therefore, the difference  $\varepsilon$  of  $L_N$  and  $L_N^*$  can be represented by Eq. (6).

$$\begin{aligned}\varepsilon(x, y) &= g(x, y) * \theta - f(x, y) * \theta = \eta(x, y) * \theta \\ &= \iint \eta(x-u, y-v) \theta(u, v) du dv.\end{aligned}\quad (6)$$

Let  $e\_max$  ( $e\_max \geq 0$ ) be the most tolerable distortion of each pixel in  $f(x, y)$ , then  $|\eta(x, y)| \leq e\_max$  if image  $g(x, y)$  can pass through the authentication. Deduced from Eq. (6), Eq. (7) is transformed into:

$$\begin{aligned}|\varepsilon(x, y)| &\leq \iint |\eta(x-u, y-v)| \theta(u, v) du dv \\ &\leq \iint e\_max \cdot \theta(u, v) du dv.\end{aligned}\quad (7)$$

According to Gaussian function [9], we get Eq. (8):

$$\iint \theta(u, v) = 1, \quad \theta(u, v) > 0.\quad (8)$$

By Eqs. (7) and (8), Eq. (9) is produced:

$$|\varepsilon(x, y)| \leq \iint e\_max \cdot \theta(u, v) du dv = e\_max.\quad (9)$$

The value of  $e\_max$  is determined by the just noticeable distortion that can be detected by human vision. The characteristic coding technique denoted by Eq. (4) corresponds to  $L_N$  quantified by 4 levels. When the pixels in  $L_N$  satisfy Eq. (10),

$$|L_N(i, j) - k \cdot 2^{P-2}| \leq e\_max, \quad 1 \leq k \leq 2^2 - 1.\quad (10)$$

The results of coding  $L_N$  and  $L_N^*$  respectively with Eq. (4) is possibly different, even if the image data alter in the tolerable range. The pixels in the shadow part of Fig. 1 totally satisfy Eq. (10).

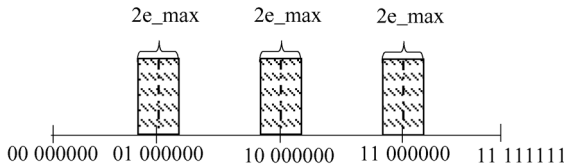


Fig. 1 Boundary effect

To solve this problem,  $L_N^*(i, j)$  is coded by  $S_3(i, j)$  and  $S_2(i, j)$  if  $L_N^*(i, j)$  is the pixel in the shadow part of Fig. 1, otherwise,  $L_N^*(i, j)$  is coded by the top two bits of  $L_N^*(i, j)$ . The code equation of characteristic value of  $L_N^*(i, j)$  is denoted as Eq. (11):

$$S_3^*(i, j) = \begin{cases} S_3(i, j), & |[S_3(i, j) 2^{P-1} + S_2(i, j) 2^{P-2}] - L_N^*(i, j)| \leq e\_max \\ x_{P-1}^*(i, j), & |[S_3(i, j) 2^{P-1} + S_2(i, j) 2^{P-2}] - L_N^*(i, j)| > e\_max \end{cases}$$

$$S_2^*(i, j) = \begin{cases} S_2(i, j), & |[S_3(i, j) 2^{P-1} + S_2(i, j) 2^{P-2}] - L_N^*(i, j)| \leq e\_max \\ x_{P-2}^*(i, j), & |[S_3(i, j) 2^{P-1} + S_2(i, j) 2^{P-2}] - L_N^*(i, j)| > e\_max \end{cases}.\quad (11)$$

### 2.3 Detail feature extraction

High resolution images  $L_1 - L_{N-1}$  represent the detail signals in different resolution. Every level component of the Laplacian Pyramid is organized to a space tree as shown in Fig. 2.

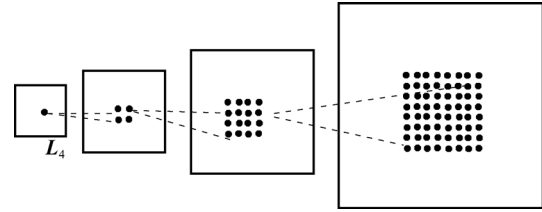


Fig. 2 Spatial relationship tree of Laplacian Pyramid

To give prominence to the significant detail properties, the detail properties of three level high frequency components are accumulated:

$$\begin{aligned}E(i, j) &= \sum_{k=0}^1 \sum_{l=0}^1 L_3(2i+k, 2j+l)^2 \\ &+ \sum_{k=0}^3 \sum_{l=0}^3 L_2(4i+k, 4j+l)^2 \\ &+ \sum_{k=0}^7 \sum_{l=0}^7 L_1(8i+k, 8j+l)^2.\end{aligned}\quad (12)$$

Code the detail signal by Eq. (13):

$$S_1(i, j) = \begin{cases} 0, & E(i, j) \geq T \\ 1, & E(i, j) < T \end{cases}\quad (13)$$

where  $T$  is a given threshold value. To filter the superfine texture, noise and other signals,  $T$  is evaluated as three times mean of  $E$ , i.e.,

$$T = \frac{3}{C_4 R_4} \sum_{i=1}^{C_4} \sum_{j=1}^{R_4} E(i, j).\quad (14)$$

Here,  $C_4$  and  $R_4$  are respectively the row number and the column number of  $L_4$ .

## 2.4 Feature similarity calculation

The top two bits of image feature  $\mathbf{S}$  reveal the primary image content, while the lowest bit represents the outstanding detail signal. Whether the image content of  $\mathbf{f}$  is consistent with  $\mathbf{g}$  can be judged by comparing their image feature. The absolute difference of  $\mathbf{S}$  and  $\mathbf{S}^*$  will be transformed into a binary image  $\mathbf{D}$ :

$$\mathbf{D}(i,j) = \begin{cases} 0, & |\mathbf{S}(i,j) - \mathbf{S}^*(i,j)| = 0 \\ 1, & |\mathbf{S}(i,j) - \mathbf{S}^*(i,j)| \neq 0 \end{cases} \quad (15)$$

Filter the noise pixel from  $\mathbf{D}$ , keep the tampering information, then get a notate image  $\mathbf{Z}$ . Morphology filter has several merits, such as small quantity of computation, fast speed, capacity of achieving the geometry and the size of objective image. Besides, it has the character of translation invariance and expandability which is convenient for multi-scale image analysis and property extraction. Because of the specialty of the morphology filter, it is adopted to filter the noise from  $\mathbf{D}$ . Morphology closing, opening and alternating filter of single structuring element cannot attend to all the image features in different directions. The original properties and edge of the objective image will possibly be harmed or damaged partly.

According to the mutual spatial relationship of image pixels, Song [10] offered a morphology filter model of multiple structuring elements with different direction properties. The model defines four kinds of lineal structures in the direction of  $0^\circ$ ,  $45^\circ$ ,  $90^\circ$  and  $135^\circ$ . This technique can protect the edge feature better when filtering noises smaller than the structure element. Consulting the multiple structuring elements filter, we extend the structuring element set in this paper. In the experiment, it is discovered that the image can be considered to be tampered if there are lines longer than 3 pixels or blocks bigger than  $2 \times 2$  in different images. Therefore, the structuring element adopted here is composed by three parts: line of 3 pixels long; block in  $2 \times 2$  size; rotation form of  $45^\circ$ ,  $90^\circ$ , and  $135^\circ$ . Tampering information  $\mathbf{Z}$  can be acquired by multiple structuring elements filter of Eq. (16) according to  $\mathbf{D}$ .

$$\mathbf{Z} = \bigcup_{i=1}^8 \left[ \bigcap_{j=1}^8 (\mathbf{D} \bullet \mathbf{K}_i) \circ \mathbf{K}_i \right], \quad (16)$$

where “ $\circ$ ” and “ $\bullet$ ” represent the morphology close and open operation respectively. The multiple structuring element sequence  $\mathbf{K}_i$  is illustrated as follows:

$$\mathbf{K}_1 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \mathbf{K}_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \mathbf{K}_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \mathbf{K}_4 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$\mathbf{K}_5 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \mathbf{K}_6 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \mathbf{K}_7 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \mathbf{K}_8 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

## 3 Authentication arithmetic

The process of sign arithmetic includes two steps:

1) Transform image  $\mathbf{f}$  by the Laplacian Pyramid, then acquire feature image  $\mathbf{S}$  by Eqs. (4) and (13).

2) Encrypt  $\mathbf{S}$  with cryptographic key, then embed it into the image  $\mathbf{f}$  as the watermark; finally, obtain the watermarked image  $\mathbf{g}$ .

The process of verification arithmetic includes four steps:

1) Extract watermark information from the tested image  $\mathbf{g}$  and encrypt it to get  $\mathbf{S}$ .

2) Transform image  $\mathbf{g}$  by the Laplacian Pyramid, then acquire the feature image  $\mathbf{S}^*$  by Eqs. (11) and (13).

3) Calculate the difference image  $\mathbf{D}$  of  $\mathbf{S}$  and  $\mathbf{S}^*$  by Eq. (15).

4) Process  $\mathbf{D}$  with the morphology filter by Eq. (16) to get  $\mathbf{Z}$ . If the value smaller than two pixels is 1 in  $\mathbf{Z}$ , the tested image can be considered as having no tampering. Otherwise, the image is tampered and  $\mathbf{Z}$  indicates the location of tampering.

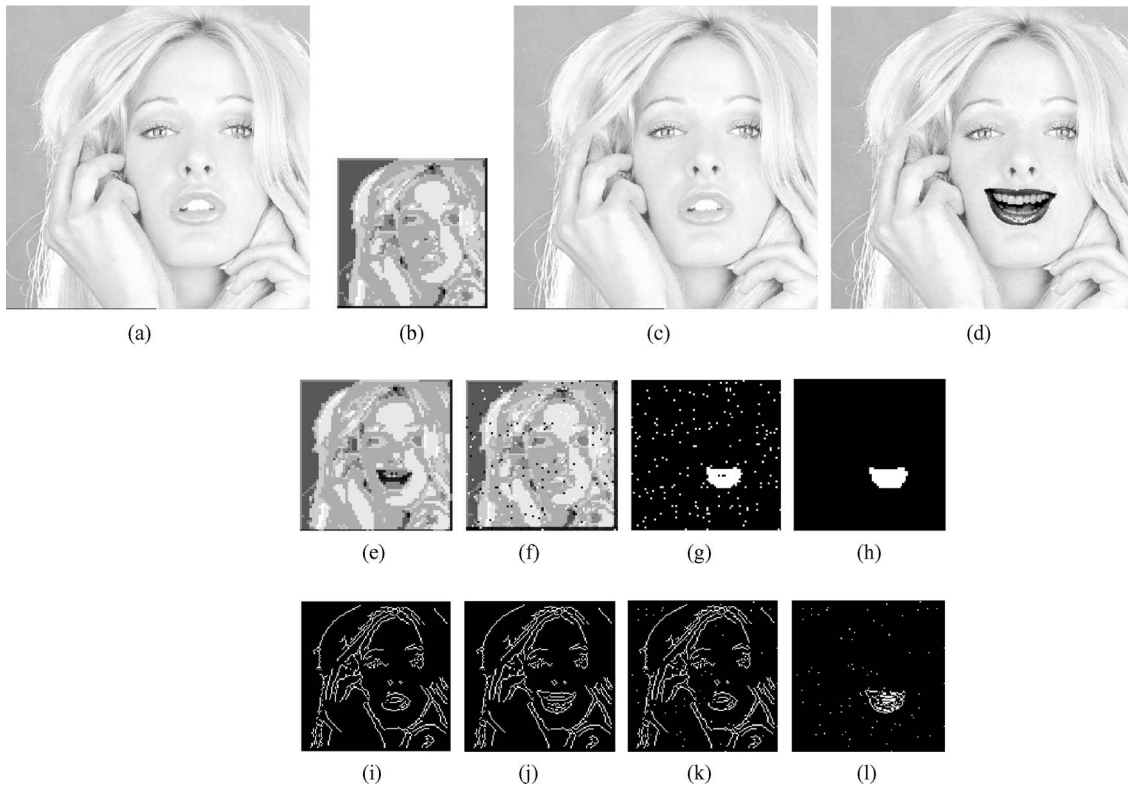
## 4 Experiment results and analysis

This algorithm fits content authentication for any gray image. In the same background, e\_max is confirmed by transforming the object's gray-scale value. After experiment, e\_max is evaluated as 16. Image tampering has two instances. One is image content tampering with edge feature change and another is image content tampering without edge feature change. As regards the former instance, techniques based on edge feature verification can detect the image tampering. As for the second instance, these techniques cannot efficiently detect image tampering.

Figure 3 is the experiment results of tampering with edge feature change. Figure 3(a) is a 256 gray-scale and  $512 \times 512$  woman image, whose feature is illustrated in Fig. 3(b). The watermarked image is illustrated in Fig. 3(c), and its peak signal-to-noise ratio (PSNR) is 36.13. Figure 3(d) is the tested image  $\mathbf{g}$ , and its feature and detected watermark are illustrated in (e) and (f) of Fig. 3 respectively. The binary difference image  $\mathbf{D}$  is Fig. 3(g), and authentication result  $\mathbf{Z}$  is illustrated in Fig. 3(h). By Fig. 3(h), we confirm that the tested image is a tampering image and the tampering location is indicated on the white zone.

Because image edge feature is changed after tampering, all techniques based on edge feature verification [3–5] can detect the image tampering and define the tampering location. Figs. 3(i)–3(l) are the experiment results of the authentication technique based on edge feature verification [5]. Tampering location information is indicated in Fig. 3(l).

Figure 4 shows the experiment result of the woman image tampered without edge feature change. Figure 4(a) is the tested image  $\mathbf{g}'$ , whose feature and watermark is

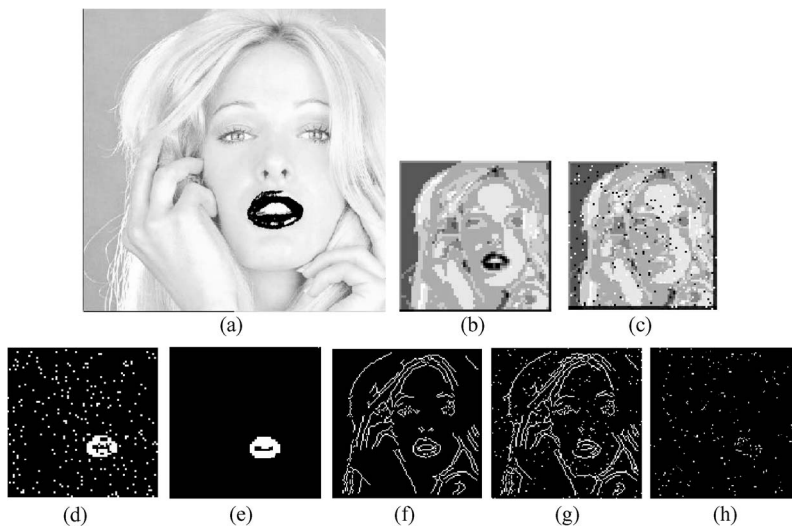


**Fig. 3** Experiment results of tampering with edge feature change. (a) Original image  $f$ ; (b) feature of  $f$ ; (c) watermarked image; (d) tested image  $g$ ; (e) feature of  $g$ ; (f) detected watermark from  $g$ ; (g) binary difference image  $D$ ; (h) authentication result  $Z$ ; (i) edge feature of  $f$ ; (j) edge feature of  $g$ ; (k) detected watermark using arithmetic of Ref. [5]; (l) authentication result using arithmetic of Ref. [5]

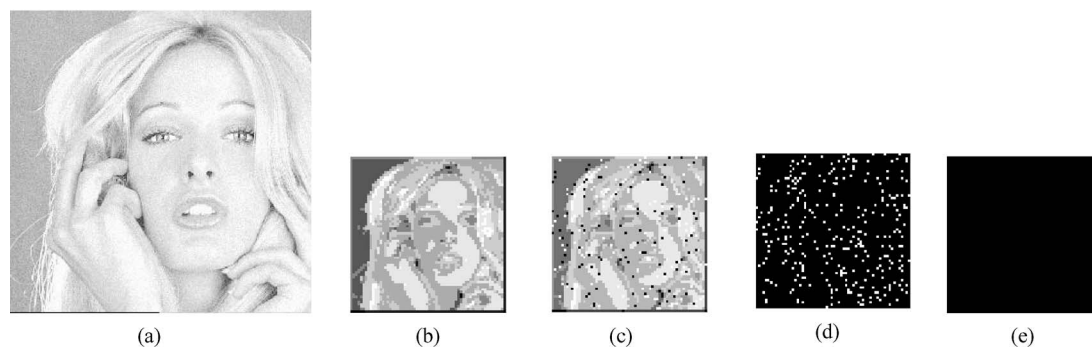
illustrated in Figs. 4(b) and 4(c). Figure 4(d) is the comparative result of the feature and the watermark of  $g'$ . Verification result (Fig. 4(e)) indicates that  $g'$  has been tampered. Figures 4(f)–4(h) are the experiment results of the authentication technique in Ref. [5]. From Fig. 4(h), we did not find any significant message. The difference between

(f) and (g) can be considered as the error caused by noise. Therefore, the tested image  $g'$  in this sense shall be improperly regarded as the original image that has not been tampered, which actually induces a miss verification.

When embedding 5% Gaussian noise in the woman image, PSNR is 28.39 (see Fig. 5(a)). The difference image



**Fig. 4** Experiment results of tampering without edge feature change. (a) Tested image  $g'$ ; (b) feature of  $g'$ ; (c) detected watermark from  $g'$ ; (d) binary difference image  $D$ ; (e) authentication result; (f) edge feature of  $g'$ ; (g) detected watermark using arithmetic of Ref. [5]; (h) authentication result using arithmetic of Ref. [5]



**Fig. 5** Experiment results of noise pollution. (a) Tested image  $g''$ ; (b) feature of  $g''$ ; (c) detected watermark from  $g''$ ; (d) binary difference image; (e) authentication result

of the feature (Fig. 5(b)) and the watermark (Fig. 5(c)) extracted from the test image  $g''$  is illustrated in Fig. 5(d). Judging by the authentication result (Fig. 5(e)), the test image has not been tampered and it will pass through the verification. It is obvious that the algorithm proposed in the paper can tolerate the noise damage. All images with a compression ratio of less than 10 can pass through the verification when compressed by JPEG. In addition, images processed by median filtering or image enhancing can pass through the verification, too.

## 5 Conclusions

A technique of image content authentication based on Laplacian Pyramid is proposed in this paper. The technique is adopted to analyze the smooth and detailed properties of the original image using Laplacian Pyramid at the sending end. Then, the features are encrypted to get a watermark and embedded in the original image. After transmission, the features are acquired in the same way from the test image and compared with the watermark extracted from the test image to obtain the difference image. According to the difference image, it can automatically figure out whether the image has been tampered or not by means of morphologic filtration and it can also pinpoint the tampering location information. Experiments prove that this technique can not only effectively detect image tampering and location information, but also tolerate some distortions produced by compression, filtration and noise degradation.

**Acknowledgements** This work was supported by the National Natural Science Foundation of China (Grant No. 60573019), Guangdong Natural Science Foundation (No. 05300198 and 05103541).

## References

1. Wong P W, Memon N. Secret and public key image watermarking schemes for image authentication and ownership verification. *IEEE Transactions on Image Processing*, 2001, 10(10): 1593–1601
2. Memon N, Vora P, Yeo B L, et al. Distortion bounded authentication techniques. In: *Proceedings of the SPIE on Security and Watermarking of Multimedia Contents II*. San Jose: SPIE, 2000, 164–174
3. Queluz M P. Towards Robust, content based techniques for image authentication. *IEEE Second Workshop on Multimedia Signal Processing*, Redondo Beach. IEEE Press, 1998, 297–302
4. Rey C, Dugelay J L. Blind detection of malicious alterations on still image using robust watermarks. *IEE Seminar on Secure Images and Image Authentication*, London. IEE Press, 2000, 7: 1–6
5. Xie L, Arce G R. A class of authentication digital watermarks for secure multimedia communication. *IEEE Transactions on Image Processing*, 2001, 10(11): 1754–1764
6. Wo Y, Han G Q, Zhang B. A new feature-based image content authentication algorithm. *Chinese Journal of Computers*, 2005, 28(1): 105–112 (in Chinese)
7. Wo Y, Han G Q, Zhang J W, et al. New image content authentication algorithm based on wavelet transform and morphologic. *Journal on Communications*, 2005, 26(8): 9–15 (in Chinese)
8. Wo Y, Han G Q. Blind watermarking algorithm based on wavelet transform and visual perception characteristics. *Journal of South China University of Technology (Natural Science Edition)*, 2005, 33(4): 29–33 (in Chinese)
9. Burt P, Adelson E. The Laplacian pyramid as a compact image code. *IEEE Transactions on Communications*, 1983, 31(4): 532–540
10. Song J, Delp E J. A generalization of morphological filters using multiple structuring elements. *IEEE International Symposium on Circuits and Systems*, 1989, 2(3): 991–994