Copy-Move Forgery Detection Based on Local Gabor Wavelets Patterns

Chao-Lung Chou[1(✉)] and Jen-Chun Lee[2]

[1] Department of Computer Science and Information Engineering,
Chung Cheng Institute of Technology, National Defense University, Taoyuan, Taiwan
chaolung.chou@gmail.com
[2] Department of Electrical Engineering, Chinese Naval Academy, Kaohsiung, Taiwan
i923002@gmail.com

Abstract. Nowadays digital images are more and more easily to be modified or tampered intentionally by most people due to the rapid development of powerful image processing software. Various methods of digital image forgery exist, such as image splicing, copy-move forgery, and image retouching. Copy-move is one of the typical image forgery methods, in which a part of an image is duplicated and used to replace another part of the same image at a different location. In this paper, we proposed a block-based passive detect copy-move forgery detection method based on local Gabor wavelets patterns (LGWP) with the advantages of high performance texture analysis of Gabor filter and rotation-invariant ability of uniform local binary pattern (LBP). Experiment results demonstrate the ability of the proposed method to detect copy-move forgery and precisely locate the duplicated regions, even when the forgery images are distorted by JPEG compression, blurring, brightness adjustment and rotation.

Keywords: Copy-move forgery · Image forgery detection
Local Gabor wavelets patterns (LGWP)

1 Introduction

Due to the rapid development of powerful image processing software, digital images are more and more easily to be modified or tampered intentionally by most people. Copy-move is one of the typical image forgery methods, in which a part of an image is duplicated and used to replace another part of the same image at a different location.

Image forgery detection is to detect whether if an image is affected by some kind of manipulations such as copy or move, image splicing and image touching. Image forgery detection techniques can be broadly categorized into active and passive approaches. The active approaches embedded additional information in an image in advance and then extracted that to discriminate its integrity. The most common methods are digital watermarks and digital signatures. The passive approach, on the other hand, is capable of detecting image manipulation without priori information. Therefore, the passive approaches are more practical in real-life applications.

S.-L. Peng et al. (Eds.): SICBS 2017, AISC 733, pp. 47–56, 2018.
https://doi.org/10.1007/978-3-319-76451-1_5

A common image forgery detection consists of four stages [1]. The first stage is typically pre-processing, in which usually including color conversion and overlap or non-overlap image partition. This stage is used to reduce the computation complexity and increase processing efficiency. The second stage is feature extraction which is to select representative image features for further discrimination. The third stage is to match extracted features in the image and determine if it is manipulated. The matching stage is either by block-based or keypoint-based. Finally, the results of tempered region will be localized and displayed.

Copy-move forgery detection techniques can be categorized into block-based and keypoint-based approaches. The block-based approach splits an image into either overlap or non-overlap blocks. Then, the features are extracted from these blocks and compared the similarity between blocks within the image. Generally, the feature extraction techniques for block-based are in the form of frequency transform, texture and intensity, and etc. Fridrich et al. [2] proposed the first block matching detection scheme based on the discrete cosine transform (DCT). Popescu and Farid [3] proposed a copy-move forgery detection method by using principal component analysis (PCA) instead of DCT. Hsu and Wang [4], Lee [5] using Gabor wavelet features to extract image block pattern information. Davarzani [6] et al. using multiresolution local binary pattern (MLBP) to extract image block pattern information. These two pattern information are known for their robustness to geometric distortions and illumination variations.

On the other hand, keypoint-based methods extract distinctive local features from entire image. Each feature is presented with a set of descriptor produced within a region around the features. Both features and descriptors in the image are classified and matched to each other to find the forgery regions. The most popular keypoint-based approaches are scale invariant feature transform (SIFT) [7, 8] and speed up robust features (SURF) [9].

In this paper, we propose a passive copy-move forgery detection method based on local Gabor wavelets patterns (LGWP). The image is converted into a gray-scale image and divided into overlapping fixed-size blocks. The proposed LGWP descriptor is applied to each block for local features extraction. The lexicographical sorting algorithm is adopted to reduce matching time while comparing image blocks features. Finally, regions of image forgery is detected through the identification of similar block pairs.

The remainder of the paper is organized as follows. In Sect. 2, the LGWP descriptor is introduced, and Sect. 3 describes the proposed method. Section 4 present the results of experiments and evaluate the performance of the proposed method. The conclusions are presented in Sect. 5.

2 Local Gabor Wavelets Patterns

Gabor filters are well-known to be particularly appropriate for texture analysis due to its similarity to those of the human visual system (HVS). Daugman [10] proposed the 2D Gabor functions by a series local spatial bandpass filters to accurate 2D space and 2D spatial frequency location. It is found that the 2D Gabor filter provide robustness

against image brightness and contrast varying and now are being used extensively in image processing applications such as iris recognition and fingerprint recognition.

The general form of a 2D Gabor filter is expressed as follows:

$$G_{\sigma,f,\theta}(x,y) = g_{\sigma}(x,y)\exp[2\pi\, if(x\, cos\theta + y\, sin\theta)] \tag{1}$$

where

$$g_{\sigma}(x,y) = \frac{1}{2\pi\sigma^2}\exp[-\frac{(\mathrm{x}^2+\mathrm{y}^2)}{2\sigma^2}] \tag{2}$$

and $J = \sqrt{-1}$, $g_{\sigma}(x,y)$ is the Gaussian function with scale parameter σ, f is the frequency parameter, θ is the orientation parameter. Let $I(x,y)$ denotes a grayscale image and $G_{\sigma,f,\theta}(x,y)$ represent a Gabor filter. The Gabor magnitude output of an image $I(x,y)$ is obtained by convolution of each block with the Gabor filter until the entire image is traversed. The magnitude responses $M_{\sigma,f,\theta}(x,y)$ of the Gabor filter can be computed as follow:

$$M_{\sigma,f,\theta}(x,y) = \sqrt{C_R^2(x,y)_{\sigma,f,\theta} + C_I^2(x,y)_{\sigma,f,\theta}} \tag{3}$$

where $C_R^2(x,y)_{\sigma,f,\theta}$ and $C_I^2(x,y)_{\sigma,f,\theta}$ denote the real and imaginary components of the discrete convolutions results of I(x, y) and $G_{\sigma,f,\theta}(x,y)$.

The local object appearance and shape can be characterized using the local magnitude directions distribution. We define $\theta_k = \frac{\pi(k-1)}{n}, k = 1,\ldots,n$ as the orientation k in total n orientations. In most cases, one would use 2D Gabor filters with eight different orientations. That is $n = 8$ and $\theta_{k=1\ldots8} = \left\{0, \frac{\pi}{8}, \frac{2\pi}{8}, \frac{3\pi}{8}, \ldots, \frac{7\pi}{8}\right\}$. Suppose there are total N sub-blocks in $I(x,y)$, the average Gabor filter respond magnitude of all directions in the same frequency and scale can be calculated as $M_{\bar{\theta}}(x,y) = \frac{1}{N}\sum M_{\theta_k}(x,y)$. The orientation that corresponds to the strongest textural information point $d(x,y)$ is defined as follows

$$d(x,y) = \arg\max_{k=1,\ldots,n}\left\{M_{\theta_k}(x,y)\right\} \tag{4}$$

The local Gabor wavelets patterns $LGWP(x,y)$ defined as follows:

$$LGWP(x,y) = \begin{cases} 1, & if\left(M_{\theta_k}(x,y) - M_{\bar{\theta}}(x,y)\right)2^{mod(n-d,k)} \geq 0 \\ 0, & otherwise \end{cases} \tag{5}$$

The modular operation in (5) is used to keep rotation-invariant textural information.

Suppose an image sub-block with $k = 8$ and $M_{\bar{\theta}}(x,y) = 100$. Figure 1(a) shows the Gabor filter respond magnitude of all 8 directions and the maxima magnitude is 167. Figure 1(b) shows the LGWP code (10001010) using (5). Notice that all points of that

Gabor filter respond magnitude greater than 100 are coded with 1. Figure 1(c) shows the image sub-block rotated 90° and Fig. 1(d) shows the corresponding LGWP code (10001010). It is obvious the LGWP code is efficient to locate the rotation and is robust to resist such attack.

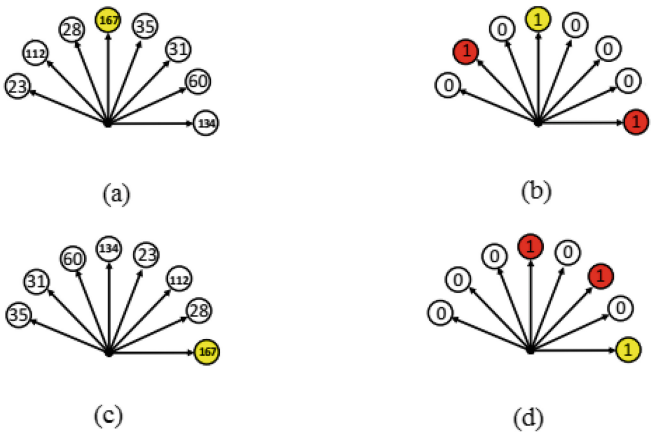


Fig. 1. Examples of LGWP code. (a) Original Gabor filter respond magnitude, (b) The LGWP code of (a), (c) Gabor filter respond magnitude after rotated 90°, (d) The LGWP code of (c).

3 The Proposed Method

In the proposed method, original image first divided into overlapping blocks of a fixed size, then the similarity of these blocks are detected, and finally displayed the possible duplicated regions. A flow-chart of the proposed forgery detection method is shown in Fig. 2.

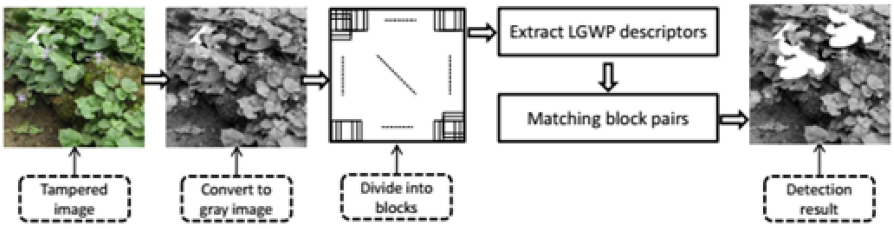


Fig. 2. The flow-chart of the proposed algorithm.

3.1 Image Pre-processing

First, the color image is converted into the gray scale image I. Then the $M \times N$ grayscale image I is divided into overlapping sub-blocks. Each block is denoted as B_{ij},

$$B_{ij}(x, y) = I(x + j, y + i) \tag{6}$$

where $x, y \in \{0, \cdots, B-1\}, i \in \{1, \cdots, M-B+1\}$, and $j \in \{1, \cdots, N-B+1\}$. Hence, the grayscale image I is divided into $(M-B+1) \times (N-B+1)$ overlapping blocks.

3.2 Feature Extraction with LGWP

In this paper, we consider 8 directions for each block. In that, total $2^8 = 256$ features can be used to represent each block. To reduce computation complexity, we using so called uniform patterns proposed by Ojala et al. [11] to extracted features from circular blocks after LGWP features extraction. A local binary pattern (LBP) is called uniform if its uniformity measure is at most 2. The 36 unique rotation invariant binary patterns that can occur in the circularly symmetric 8 neighbors as shown in Fig. 3. By applying uniform local binary pattern, the LGWP feature vector can efficient reduced from 256 to 36 and maintain rotation-invariant ability at the same time.

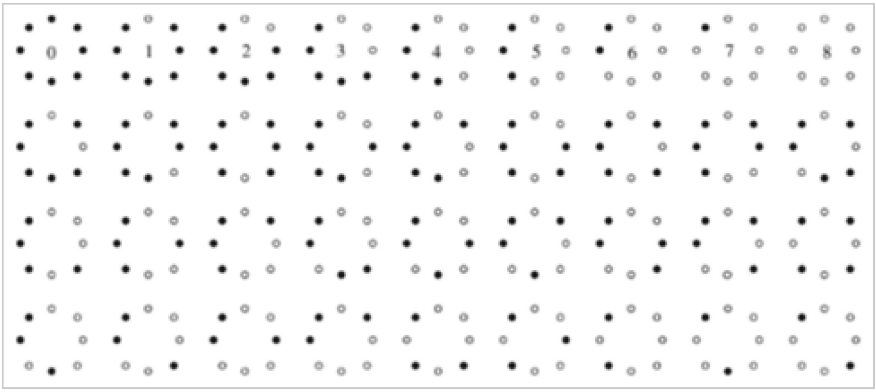


Fig. 3. The 36 unique rotation invariant binary patterns that can occur in the circularly symmetric 8 neighbors [11].

3.3 Matching Block Pairs

The matching techniques enhances the computational complexity during the search of identical values in a large size image. For block-based image forgery detection, sorting, hash, correlation and Euclidean distance are most common approaches [1]. In this paper, we use the lexicographical sorting technique to detect potentially tampered region through the adjacent identical pairs of blocks. The similar feature vectors are stored in neighboring rows after lexicographical sorting, such that the features of duplicated block pairs appear successively. The blocks were compared using Euclidean distance as follows:

$$B_{\text{distance}}\left(\widehat{V}_i, \widehat{V}_{i+j}\right) = \sqrt{\left(x_i - x_{i+j}\right)^2 + \left(y_i - y_{i+j}\right)^2} \tag{7}$$

where (x, y) is the center of the corresponding block and $\widehat{V}_i$, $\widehat{V}_{i+j}$ are sorted adjacent feature vectors derivative from original feature vector $V_i = (f_1, f_2, \ldots, f_{36})$.

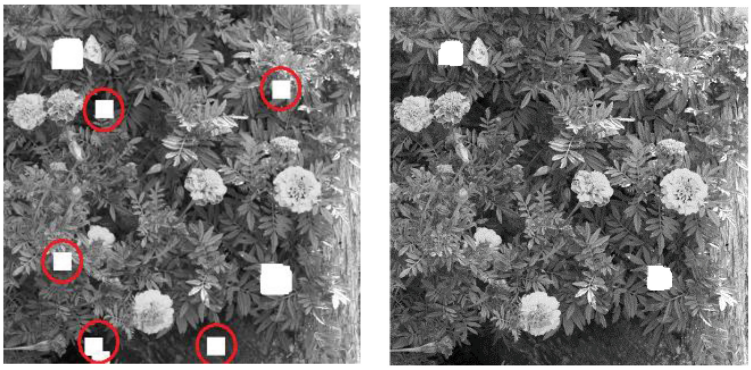
The more similar between blocks, the smaller value of $B_{\text{distance}}\left(\widehat{V}_i, \widehat{V}_{i+j}\right)$ is calculated. Hence, a predefine threshold T_s is given to indicate their similarity. We define (i) is the smallest distance between the ith and the nearby features in vector $\widehat{V}_i$ lower than T_s as follows:

$$D(i, \sigma) = min\{D(i;i-j), \ldots, D(i;i-1), D(i;i+1), \ldots, (i;i+j)\} \tag{8}$$

In addition, there is high possibility that the similarity of nearby blocks feature vectors is very close. Thus, we compared only blocks in which the position distance from other blocks exceeds distance threshold T_d.

3.4 Post-processing

Generally, all detected blocks, including the original and forged blocks, are marked into white (pixel value = 255) to generate the detection result. Figure 4(a) shows an example of the early detection results with some distortion (marked in red circle). To obtain accurate forgery regions, all blocks are further calculated their pairwise alike based on the area of these blocks using 4-connected components labeling method. The difference Fig. 4(b) shows the final detection results after post-processing from Fig. 4(a).



(a) (b)

Fig. 4. Examples of detection results, (a) early results with distortions, (b) final results after post-processing.

4 Experimental Results

In the experiments, the proposed method is evaluated using publicly available CoMoFoD database [12]. The database consists of 260 forgery images with two different

sizes 512 × 512 and 3,000 × 2,000. Here, we use the 512 × 512 size for all experiments. Images are grouped into 5 groups of manipulation: translation, rotation, scaling, combination and distortion. Different types of post-processing methods, such as JPEG compression, blurring, noise adding, color reduction etc., are applied to all forged and original images.

All experiments were performed on a personal computer with a 3.2 GHz CPU, 4 GB memory, with MATLAB 8.5 environment. To illustrate the performance of the proposed algorithm, we referenced correct detection ratio (CDR) indicates the performance of the algorithm in terms of accurately locating the pixels of copy-move regions in the tampered image defined as follows:

$$\text{CDR} = \frac{\textit{The detected tampered region}}{\textit{The tampered region}} \tag{9}$$

At first, we test the detection performance without post-processing. Figure 5 shows the example of detection results.

The statistical detection rates without post-processing for sub-blocks of various sizes of 16 × 16, 32 × 32, and 48 × 48 are presented in Table 1. The proposed method performs well in blocks sizes of 16 × 16 than other size because some portions of the forged regions are so small that they cannot be detected when using larger block sizes. Thus, we use the block size at 16 × 16 for further experiments.

The ability to resist post-processing attacks is fundamental to copy-move forgery detection methods. The most common post-processing attacks are JPEG compression, brightness adjustment, blurring and rotation. To evaluate the robustness and effectiveness of the proposed method in resisting above post-processing attacks, the experimental results were compared with [5] in JPEG compression (quality factor = 20, 30, 50, 70, 90), brightness adjustment ([0.01, 0.95], [0.01, 0.90] and [0.01, 0.8]), Gaussian blurring ($\sigma^2 = 0.005$ and 0.0005) and rotation (0^o, 2^o, 20^o, 45^o, 60^o, 90^o, 150^o and 180^o) showing in Table 2.

As shown in Table 2, the proposed algorithm achieved high correct detection ratios for JPEG compression with a quality factor above 70 and also provides excellent robustness against changes in image brightness, as evidenced by the reliable detection performance achieved in the [0.01, 0.8] range.

The forged images blurring using Gaussian blurring with standard deviation equals 0.005 and 0.0005. Both detection results are in high performance.

The case in which the forged images regions is copied, rotated and moved to another position in the same image without distorting it using any other techniques. The duplicated regions are rotated by angles selected with 0^o, 2^o, 20^o, 45^o, 60^o, 90^o, 150^o and 180^o. Figure 6 shows the examples of image with different rotating angles. As Table 2 shows, the proposed method is robust against rotation attack at different rotating angles and outperformed [5].

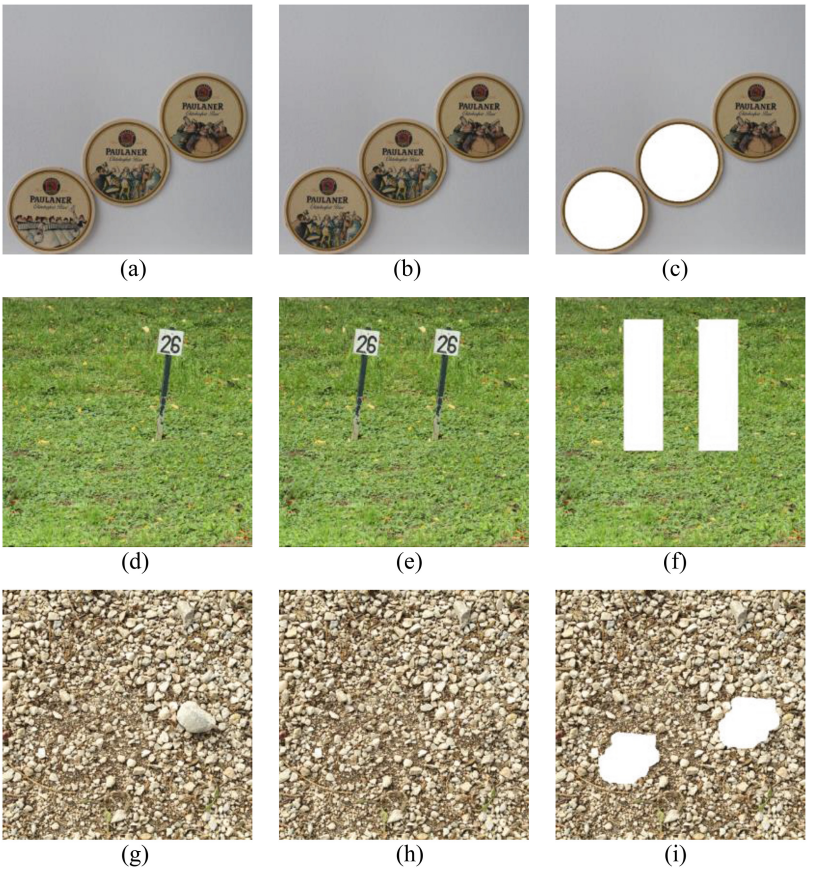


Fig. 5. Detection results without post-processing (a), (d), (g) original image, (b), (e), (h) forgery image, and (c), (f), (i) detection results.

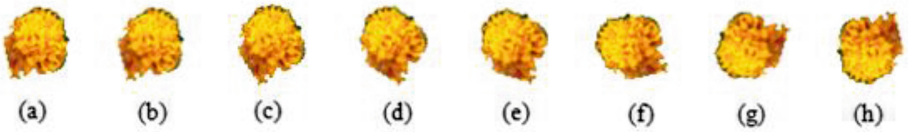


Fig. 6. Examples of rotation attacks for a copy-move forgery region (a) original (b) 2° (c) 20° (d) 45° (e) 60° (f) 90° (g) 150° (h) 180°.

Table 1. Copy-move forgery detection results of the proposed method without post-processing.

Block size	CDR
16 × 16	0.991
32 × 32	0.974
48 × 48	0.967

Table 2. Comparison of detection results of forged images by JPEG compression, brightness adjustment, gaussian blurring and rotation.

Post-processing attacks		The proposed method	[5]
JPEG compression (Quality factor)	90	0.975	0.970
	70	0.910	0.920
	50	0.862	0.840
	30	0.570	0.520
	20	0.350	0.320
Brightness adjustment	[0.01, 0.95]	0.990	0.986
	[0.01, 0.90]	0.990	0.975
	[0.01, 0.80]	0.990	0.953
Gaussian Blurring (σ^2)	0.005	0980	0.976
	0.0005	0.958	0.946
Rotation angles	0^o	0.991	0.988
	2^o	0.942	0.93
	20^o	0.830	0.12
	45^o	0.910	N/A
	60^o	0.810	0.09
	90^o	0.991	N/A
	150^o	0.840	N/A
	180^o	0.991	0.38

5 Conclusions

Image forgery detection is a rapidly growing research area, especially on passive techniques. Block-based approach is more popular approach due to its suitability with various feature extraction techniques and the capability to achieve a high matching performance. In this paper, we proposed a passive block-based image copy-move forgery detection method based on local Gabor wavelets patterns (LGWP) with the advantages of high performance texture analysis of Gabor filter and rotation-invariant ability of uniform local binary pattern (LBP). Experiment results demonstrate the efficacy and robustness of the proposed algorithm in detecting copy-move forgery, while forgery images is under JPEG compression, brightness adjustment, blurring, and rotation.

References

1. Warif, N.B.A., Wahab, A.W.A., Idris, M.Y.I., Ramli, R., Salleh, R., Shamshirband, S., Choo, K.-K.R.: Copy-move forgery detection: survey, challenges and future directions. J. Netw. Comput. Appl. **75**, 259–278 (2016)
2. Fridrich, J., Soukal, D., Lukas, J.: Detection of copy–move forgery in digital images. In: Proceedings of Digital Forensic Research Workshop, pp. 19–23 (2003)
3. Popescu A., Farid, H.: Exposing digital forgeries by detecting duplicated image regions. Technical report TR2004-515, Department of Computer Science, Dartmouth College (2004)
4. Hsu, H.C., Wang, M.S.: Detection of copy-move forgery image using Gabor descriptor. In: Proceedings of International Conference on Anti-Counterfeiting, Security and Identification (ASID), pp. 1–4 (2012)
5. Lee, J.-C.: Copy-move image forgery detection based on Gabor magnitude. J. Vis. Commun. Image Represent. **31**, 320–334 (2015)
6. Davarzani, R., Yaghmaie, K., Mozaffari, S., Tapak, M.: Copy-move forgery detection using multiresolution local binary patterns. Forensic Sci. Int. **231**, 61–72 (2013)
7. Amerini, I., Ballan, L., Caldelli, R., Bimbo, A.D., Serra, G.: A SIFT based forensic method for copy-move attack detection and transformation recovery. IEEE Trans. Inf. Forensics Secur. **6**(3), 1099–1110 (2011)
8. Christlein, V., Riess, C., Jordan, J., Riess, C., Angelopoulou, E.: An evaluation of popular copy-move forgery detection approaches. IEEE Trans. Inf. Forensics Secur. **7**(6), 1841–1854 (2012)
9. Bo, X., Junwen, W., Guangjie, L., Yuewei, D.: Image copy-move forgery detection based on SURF. In: Proceedings of International Conference on Multimedia Information Networking and Security, pp. 889–892 (2010)
10. Daugman, J.: Two-dimensional analysis of cortical receptive field profiles. Vision. Res. **20**, 846–856 (1980)
11. Ojala, T., Pietikainen, M., Maèenpaèa, T.: Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Trans. Pattern Anal. Mach. Intell. **24**(7), 971–987 (2002)
12. CoMoFoD database Homepage. http://www.vcl.fer.hr/comofod. Accessed 23 Oct 2017