# A Novel Keypoint Based Forgery Detection Method Based on Local Phase Quantization and SIFT

Beste USTUBIOGLU[1], Gul MUZAFFER[1], Guzin ULUTAS[1], Vasif NABIYEV[1]and Mustafa ULUTAS[1]

[1]Departmant of Computer Engineering, Karadeniz Technical University, Trabzon, Turkey
bgencturk@ktu.edu.tr, gulmuzaffer@ktu.edu.tr, guzin@ieee.org, vasif@ktu.edu.tr, ulutas@ieee.org

## Abstract

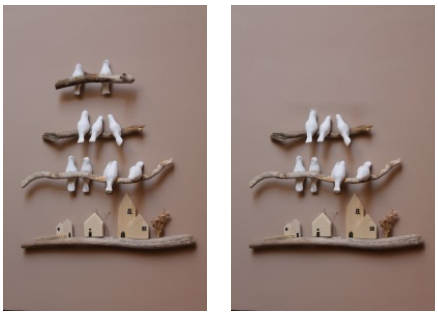
**Increase on the availability of the image editing software makes digital image forgery serious problem. Researchers proposed methods to cope with image authentication in recent years. We proposed a novel keypoint based passive image authentication technique to determine the copy move forgery. The method extracts the structural texture information from the test image by using LPQ (Local Phase Quantization) operator to make the keypoint extraction techniques more successful. SIFT is used extract the keypoints from texture image. Forged regions are detected by matching the keypoints. The method also improves the keypoint based passive image authentication mechanism by extraction texture information before keypoint extraction. Experimental results show that, the method detects forged regions on the images even if the forged image has undergone some attacks (Gaussian blurring/Additive White Gaussian Noise) and jpeg compression).**

## 1. Introduction

Digital media such as images or videos become widespread by means of the low cost digital cameras and cell phones in nowadays. Images or videos are widely used in many areas, such as medical imaging, journalism, criminal and forensic investigations. However, digital images can be easily modified without leaving visible clues due to the sophisticated editing software (for example, Photoshop, 3D Max, GIMP). Thus, approving the fidelity of digital media is a challenging problem. Researchers suggest techniques to examine the originality of digital images or videos. Techniques reported in the literature can be roughly divided active and passive methods.

Active methods such as digital watermarking or digital signatures require additional information to be transmitted and they also need key management procedures. On the contrary, passive methods can authenticate an image without any additional information or specialized hardware. The advantages of the passive methods make them popular to researchers in recent years.

Copy move forgery is one of the most popular forgery techniques since even a beginner can make this forgery by freely available image editing tools. A part of an image is copied and pasted into another region in the same image to hide some of the objects or emphasize a particular object in the image. But detecting the same regions is very difficult, because the copied regions usually are processed by some operations such as blurring, noise addition, compression and geometrical distortion. Thus, forgery detection method should detect the replicated regions, even if they are slightly different from each other. Original image and example of copy move forgery image given in Fig. 1 (a) and (b) respectively.



(a) (b)

**Fig. 1.** (a) Original image (b) Forged image

Passive image authentication methods in the literature can be divided into two groups: Block based and Keypoint based methods. Fridrich et al.s work is the first attempt in the literature to detect the copy move forgery operation [1]. Their method is block based and not robust to against some post processing operations such as scaling, translation and rotation. After this work, Popescu et al. used PCA to extract feature vectors from the blocks [2]. Their work decreased the dimension of feature vector utilizing the characteristic of PCA. The method is more robust to additive noise. But their method has also a drawback: it cannot detect forgery if copied region is rotated before it is pasted. Bayram et al. suggested using Fourier-Mellin Transform (FMT) to create the feature vectors [3].

After this works, keypoint based methods were proposed to overcome the rate complexity of block based method. Huang proposed the algorithm based on SIFT (Scale Invariant Feature Transform) [4], and subsequently, Amerini et al improved the SIFT approach by adding the use of hierarchical clustering on the SIFT key points [5]. Their method is robust to rotation and scaling but cannot detect forgery by smooth surfaces.

Block and keypoint based techniques do not work properly if one copies a smooth region of the image and pastes it on another region to hide a clue as a forgery. Since block based methods divide input image into overlapping blocks and use threshold to judge similarity among group of blocks, large number of similar group of blocks (eg. two groups of blocks corresponding to sky in the image) must be ignored to deal with false negatives. Therefore, these methods cannot detect forgery if forged region is smooth or have no texture. Likewise, keypoint based authentication methods cannot detect smooth forged regions because keypoint extraction algorithms extract keypoints from complex regions.

We proposed a method based on LPQ and SIFT. Our method extracts structural texture information from the forged image as

the first step to use keypoint extraction methods on them. Seemingly smooth regions of images also have a texture (due to sensor and/or quantization noise) and the proposed method reveals the structure of these regions by using the Local Phase Quantization (LPQ) operator. Thus, keypoint extraction algorithms can obtain keypoints from the textural information of the image. Copy-paste regions are detected by matching the keypoints. Experimental results show that the method gives higher detection ratios, especially smooth surfaces, compared to SIFT based works in the literature [5]. The rest of the paper is organized as follows. Section 2 gives proposed work with a brief introduction to LPQ and SIFT approach. The experimental results and conclusions are given in Section 3 and Section 4 respectively.

## 2. Proposed Work

The proposed method consists of three stages: (i) extraction of the texture information from image using LPQ, (ii) detection of the SIFT keypoints from the LPQ image and (iii) matching the keypoints to detect tampered regions. The details of the method are given in the subsections below.

### 2.1. Image Texture Feature Extraction using LPQ

Proposed method reveals the structural texture information from the forged image by using the LPQ operator. Thus, SIFT can obtain keypoints from the textural information of the image.

The Local Phase Quantization (LPQ) operator was originally proposed by Ojansivu and Heikkila as a texture descriptor [6]. LPQ is proposed as a spatial blurring based on quantized phase information of the Discrete Fourier Transform (DFT).

The blurring in spatial domain is represented by a convolution between the image intensity and a point spread function(PSF).In frequency domain this equal to $G=F*H$ where $G$, $F$ and $H$ are the discrete Fourier transforms (DFT) of the blurred image, original image, and the PSF in order of. Additionally taking into account only the phase of the spectrum the relation become a sum $\angle G(u) = \angle F(u) + \angle H(u)$ . It is assume that the blur PSF h(x) is centrally symmetric, so $h(x)=h(-x)$, its Fourier transform is all time real-valued, and as a result its phase is just a two-valued function, given by $\angle H(u) \in (0,\pi)$. The shape of H for regular PSF make that at least the low frequency values of H are positive. At these frequencies, $\angle H = 0$ subject to , $\angle F$ to be a blur invariant property.

In LPQ, the phase is analyzed in local neighbourhoods $Nx$ for each pixel position x of the image $f(x)$. The local frequency characteristics can be obtained using selective frequency filters. The lower frequency resolution depict higher spatial resolution. The low frequency phase angles are indicated to be invariant to centrally symmetric blur. These local spectra are figured out using a short term Fourier transform (STFT) defined by

$$F(u,x)=\sum_{y\in N_x} f(x-y)e^{-j2\pi u^T y} \quad (1)$$

We set $m$ value to 9. Where $x\in\{x_1,x_2,\ldots x_N\}$ compose of simply 1-D convolution for the rows and columns respectively. The local Fourier coefficients are computed at four angles $[0, \pi/2, \pi, 3\pi/2]$ equal to 2-D frequencies $u1 = [a,0]^T$, $u2 = [0,a]^T$ ,$u3 = [a,a]^T$, and $u4 = [a,-a]^T$ where $a = 1/m$, (m is window size) is a small enough scalar to satisfy $H(u_i) > 0$. We set $m$ value to 9. The local Fourier coefficients are computed at four angles $[0, \pi/2, \pi, 3\pi/2]$ corresponding to 2-D frequencies $u1 = [a,0]^T$, $u2 = [0,a]^T$ ,$u3 = [a,a]^T$ and $u4 = [a,-a]^T$ where $a = 1/m$, (m is window size) is a sufficiently small scalar to satisfy $H(u_i) > 0$. For each pixel position this results in a vector:

$$F_x^c=[\{F(u_1,x),F(u_2,x),F(u_3x),F(u_4,x)\}] \quad (2)$$

$$F_x= [\text{Re}\{F(x), \text{Im}\{F(x)\}]^T \quad (3)$$

where $Re\{\cdot\}$ return real parts of a complex number and $Im\{\cdot\}$ return imaginary parts of a complex number.

Then, $G_x$ is computed for pixel and the resulting vectors are quantized using a simple scalar quantizer:

$$q_j = \begin{cases} 1 \text{ if } g_j \geq 0 \\ 0 \text{ otherwise} \end{cases} \quad (4)$$

where $g_j$ is the jth component of the vector $G(x) = [Re\{F(x), Im\{F(x)\}]$ . Finally, the label image $f_{LPQ}(x)$ is resulted eight binary coefficients $q_j(x)$ are represented as integer values between 0-255 using binary coding:

$$f_{LPQ}(x) = \sum_{j=1}^{8} q_j 2^{j-1} \quad (5)$$

The diagram of the computing LPQ as can be seen in Fig 2. We used LPQ to extract LPQ(texture) image. Fig. 3 shows the LPQ image of Fig. 1. (b).

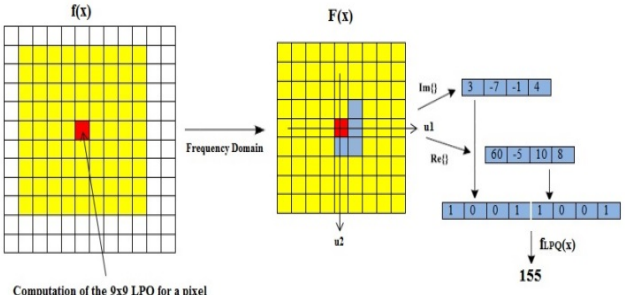



**Fig. 2.** A summary of LPQ method

**Fig. 3.** LPQ image

### 2.2. Detection SIFT Keypoints from the LPQ Image

The proposed method extracts keypoints from the LPQ image using Scale Invariant Feature Transform proposed by Lowe et al. in 2004 [7]. Scale-space extrema detection, keypoint

localization, orientation assignment and determination of the keypoint descriptors are the steps of the SIFT. First, scale space is constructed to detect the local interest points called keypoints. Potential keypoints are searched over all scales. Variable scale Gaussian function $G(x,y,\sigma)$ convolved with an input image $I(x,y)$ to construct the scale space function. Scale space of an image $L(x,y,\sigma)$ is calculated as in (6).

$$L(x,y,\sigma)= G(x,y,\sigma)* I(x,y) \quad (6)$$

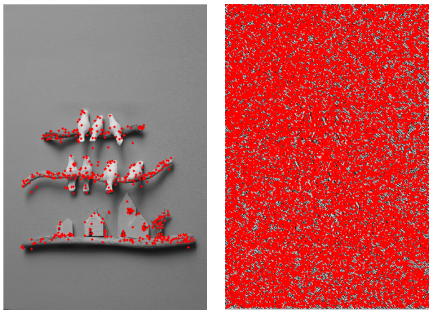
The difference between two nearby scaled images separated by a multiplicative factor k, is convolved with the image $I(x,y)$ as in (7) to extract stable keypoint location.

$$D(x,y,\sigma)= L(x,y,k\sigma)-L(x,y,\sigma) \quad (7)$$

Keypoint localization is the next step during the algorithm. Each point in D is compared with its 8 neighboring pixels and 9 pixels in neighboring scales. If the center value is the minimum or maximum, this point is an extrema and it is a potential keypoint. Each keypoint is assigned to an orientation to achieve rotation invariance. A neighborhood of each keypoint is taken according to scale to judge the orientation. Gradient magnitude and direction is calculated in that neighborhood.

Keypoint descriptors are created as the last step. A *16×16* pixel neighborhood around the keypoint is taken and this region is divided into *4×4* pixel subblocks. 8-bin orientation histogram is constructed for each subblock. 128 bin values are obtained from all subblocks and they are represented as a vector to form keypoint descriptor.

Fig 4. (a) and (b) shows extracted keypoints from of Fig. 1. (b) and from Fig. 3 respectively. SIFT cannot find keypoints on the wall since the wall has smooth surfaces as can be seen Fig. 4. (a). However, SIFT extracts a lot of keypoints from the texture image of the same image as given Fig. 4 (b). Structural texture information causes the increase on the number of keypoints and matched keypoints as shown in the results.Thus, our methos extract texture information from the image before keypoint extraction.



(a) (b)

**Fig. 4.** SIFT keypoints extracted from (a) forged image (b) texture image

## 2.3. Matching the Keypoints

The proposed method uses the approach defined in [5] to judge similar keypoints. Keypoint matching algorithm defined by Amerini et al. is applied for a keypoint descriptor as explained below.

1. Dot products are calculated between current keypoint descriptor and the others, *{d1⋯dn}*.

2. Dot product angles are computed by inverse cosine, and then sorted and dot product values and their corresponding indexes are stored.

3. The ratio of two neighbors, *(di, d(i+1)),* is compared with a predefined threshold t until the ratio is greater than t. Assume that the procedure stops at kth index, keypoints corresponding to *{di ⋯ d(i+k)}* are considered as match for the current keypoint. We set *t* value to 0.6.

The procedure defined above is applied to all keypoints. Matched keypoints designate forged regions and provide information about the authenticity of the image.

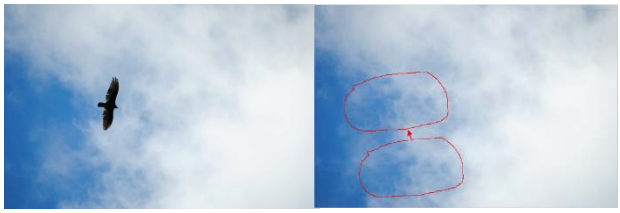
## 3. Experimental Results

This section gives the detailed analysis to show the effectiveness of the method. The forged images were created by an open source image editing software, GIMP, using images of size *640x420* pixels and *1200x800* pixels from Google image search. Border smoothing is also applied to all forged images during forgery to hide the clues on the peripheral of the covered area. Forgery detection capability of the proposed method for a *N×M* test image is evaluated using a metric called by Detection Ratio (DR) given in (8). *DR* is the ratio of matched keypoints inside tampered regions, $K_F$, to the total number of pixels, *F*, that reside on those regions. Independence from image size is ensured by multiplying these metric by *NM/100*. Higher DRs correspond to better accuracy in detecting forged regions.

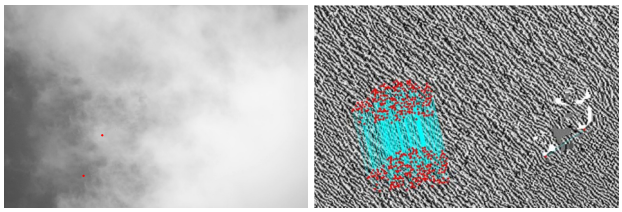
$$DR = \left(\frac{K_F}{|F|}\right)\frac{NM}{100} \quad (8)$$

The first experiment, two different types of attacks are applied on the image to create the forged versions: Simple and multiple attacks. Fig. 5(b) is an example of a simple attack. A region with a bird on the image given in Fig. 5(a) is covered by another smooth region from the same image to create the forged image given in Fig. 5(b). Fig. 5(c) shows that SIFT [5] detects 2 keypoints on the forged regions since the region is covered by smooth region and any of them is matched. However, the proposed method finds 11600 keypoints on the forged image and matches 412 of them as can be seen in Fig. 5(d). The proposed method reveals the forged region with more matched keypoints. When the forgery operation hides a portion of the image with a smooth region, other SIFT do not find any keypoints in forged regions.

Multiple attack is used to create more than one forged regions on the image. Butterfly region on the image given in Fig. 6(a) is copied and pasted on the other two regions on the same image as indicated by the red arrows to create the forged one given in Fig. 6(b). The total matched keypoints and keypoints for proposed method and SIFT [5] are (858, 359) and (15922, 2520) respectively as given in Fig. 6(c) and 6(d). The proposed method finds more keypoints on the forged regions even if the the copied region is complex region compared with SIFT.



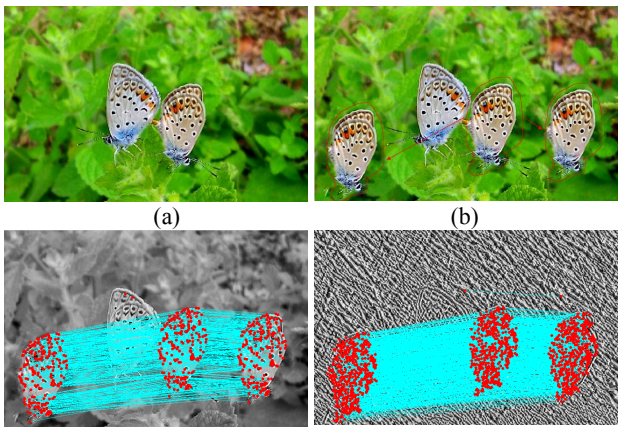
(a) (b)



(c) (d)

**Fig. 5.** (a) Original image (b) Forged image (c) The result of SIFT method (Total keypoints: 2 Matched keypoints: 0)(d) The result of proposed method(Total keypoints: 11600 Matched keypoints: 412)

Blurring operation is used in the second experiment to blur the forged image. The red circle pattern given in Fig. 7(a) is duplicated to create forged image, Fig 7(b). The forged image is blurred by a Gaussian filter with parameters $(windows\ size, w = 9\ \sigma = 9)$. Proposed method and SIFT [5] detect 5153, 1163 total number of keypoints respectively. The matched keypoints are seen in Fig. 7(c), 7(d) as 1789,637 respectively. The proposed method has higher accuracy compared to SIFT even though with larger blurring radius.

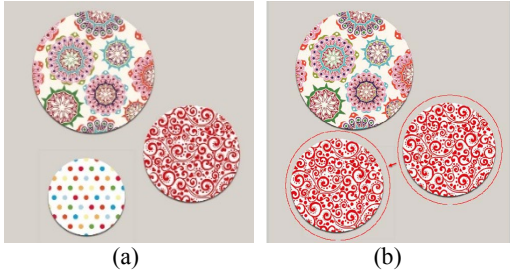


(a) (b)

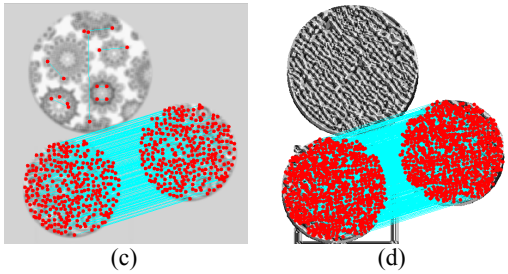
(c) (d)

**Fig. 6.** (a) Original image (b) Forged image (c) The result of SIFT method (Total keypoints: 2520 Matched keypoints: 359)(d) The result of proposed method(Total keypoints: 15922 Matched keypoints: 852)

50 test images of size *640x420* pixels are blurred using the following parameters: $\sigma = 5$, $\sigma = 7$ *and* $\sigma = 9$ for *5x5*, *7x7* and 9x9 kernels. Figure 8 gives the average detection ratios of the methods. The results are also compared with SIFT [5] as can be seen in Fig 8. The proposed method has higher *DR* compared to SIFT.



(a) (b)



(c) (d)

**Fig. 7.** (a) Original image (b) Forged image (c) The result of SIFT method (Total keypoints: 1163 Matched keypoints: 637)(d) The result of proposed method (Total keypoints: 5153 Matched keypoints: 1789)

Another experiment is realized to show the effectiveness of the method under Additive White Gaussian Noise operation. For this purpose, *30 dB 45 dB* and *60 dB* signals are used to hide the clues of the forgery operations on the 50 forged images. Fig. 9 shows average *DR* of the method and SIFT. The method yields higher average *DR* compared to SIFT as shown in the bar chart.

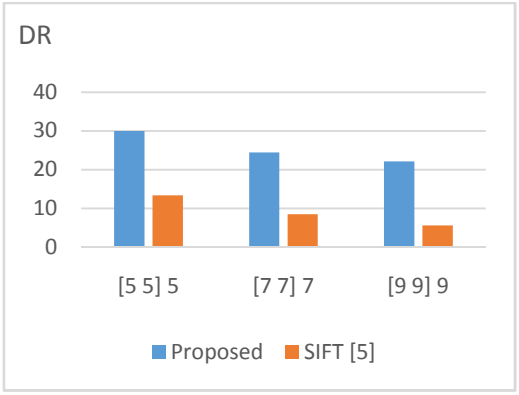



**Fig. 8.** Comparison test results for Gaussian Blurring

In the last experiment, 40 tampered images of size *1200x800* pixels were distorted by JPEG compression with different quality factors QF=90, 80 and 70. Fig. 10 indicates that the proposed method yields higher average DR compared to SIFT for jpeg compression.


**Fig. 9.** Comparison test results for AWGN

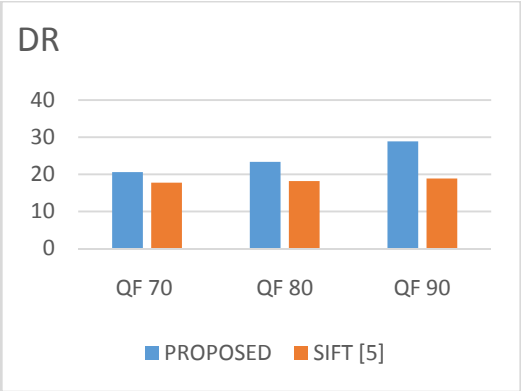



**Fig. 10.** Comparison test results for JPEG compression

## 4. Conclusions

A novel keypoint-based image authentication scheme is proposed for copy move forgery detection in this work. Since keypoint based techniques make use of structural information such as image texture, they cannot detect forgery on the smooth regions. The proposed method is based on keypoint selection and uses LPQ before SIFT to emphasize texture information. LPQ extracts texture information from images with seemingly smooth regions. Thus, keypoint extraction algorithms are applicable on the structural information and extract keypoints from the structural information of the smooth regions. Thus, one of the most important disadvantages of the keypoint based passive authentication mechanisms reported in the literature is eliminated by the proposed method.

## 5. References

[1] J. Fridrich, "Detection of copy-move forgery in digital images", Digital Forensic Research Workshop, Cleveland, OH, pp. 19–23, 2003.

[2] A. C. Popescu, H. Farid, "Exposing digital forgeries by detecting duplicated image regions", Tech. Rep. TR2004-515, Department of Computer Science, Dartmouth College, 2004.

[3] S. Bayram, H. Sencar, N. Memon, "An efficient and robust method for detecting copy-move forgery", IEEE International Conference on Acoustics, Speech and Signal Processing, 2009.

[4] H. Huang, W. Guo, and Y. Zhang, "Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm," in Proceedings of IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol. 2, 2008, pp. 272-276.

[5] I. Amerini, L. Ballan, R. Caldelli et al "A SIFT-based forensic method for copy–move attack detection and transformation recovery". IEEE Trans Inf Forensic Secur 6:1099–1110. doi:10.1109/TIFS.2011.2129512.

[6] J. H. Ville Ojansivu, "Blur Insensitive Texture Classification Using Local Phase Quantization", Image and Signal Processing, pp. Volume 5099, 2008, pp 236-243, 2008.

[7] G. Lowe SIFT - The Scale Invariant Feature Transform. Int J. 2004;2:91–110.