Research Journal of Recent Sciences _____ ISSN 2277-2502
Vol. **1(12),** 1-6, December **(2012)** *Res.J.Recent Sci.*

Image Duplication Forgery Detection using Two Robust Features

Mohamadian Zahra
Department of Computer engineering, Shahrood Branch, Islamic Azad University, Shahrood, IRAN

Available online at: www.isca.in
Received 17th August 2012, revised 27th August 2012, accepted 29th August 2012

Abstract

Nowadays duplication forgery is the most applicable method to make tampered images. This method copies a region of an image and pasted into another part(s) of that image. There are several methods to detect forged images. Most of them can only detect those regions which are exactly pasted into another part, but in practice the copied region is scaled or rotated before pasting to achieve the best matching with surrounding. In this paper we propose a method to detect duplicated regions in an image using SIFT features and then using Zernik moments. By using SIFT features we can detect duplicated regions even if they scaled or rotated, but these features cannot find flat duplicated regions. Zernik moments can solve this problem; they can find flat copied regions but failed to find scaled copied regions. So at first we will apply SIFT feature extraction method and find SIFT key points, but there is no SIFT key points in flat regions, then we will apply zernik moments on such regions, So duplicated region in all over the image even in flat regions will detected while the process time is efficient.

Key words: Duplication forgery, Zernike moments, SIF, scaling, rotating, flat region.

Introduction

Nowadays wide use of Internet and digital images in it, have made these images source of information[1,2], in courts they may be used as testimony to proof or refuse evidences, and also a number of tampered images have been published by major newspapers. Otherwise "Communication is not only a system of information, but also an integral part of education and development" [3] and there are lots of images in such fields, so authenticating such images is very important.

There are several methods to make forged images, such as[4]:

Removing: operations that remove some parts from the multimedia content.

Replacement: operations that replace some parts of multimedia content with parts borrowed from other content. One example is: Replacing a person's face in a photo with one from another photo.

Copy-move: operations that copies a part of an image and pasted it into another part of it.

Photomontage: operations that combine several pictures, producing a new one of high quality.

Computer-Generated Media: media content generated by computers, e.g., computer graph, speech synthesis, and computer-aided drawing.

Among all of these methods copy-move is the most common approach to make forged images. In figure-1 you can see a kind of copy-move forgery.

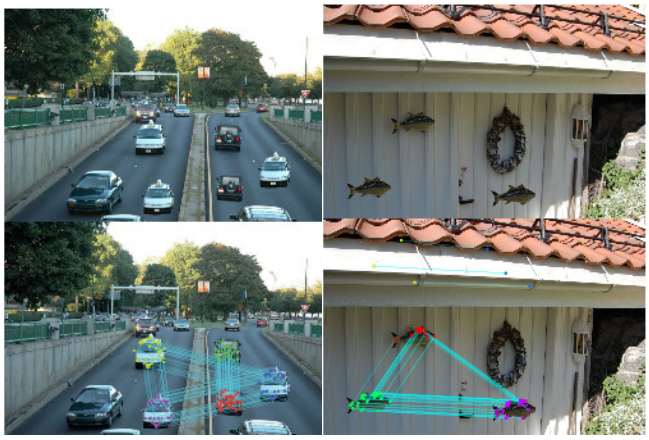


Figure-1
Examples of copy-move forgery, The first row is the forged image, and the second row is detected copied regions[19]

There are some approaches in the literature to detect copy-move forgery[5]. All of these methods can detect the copy-move forgery without any rotation or modification the scale of copied region before pasting.

In practice the copied region is scaled or rotated so that the image seems more natural you can see an example of these modifications in figure-2. Such modifications changes pixel values [5] so these methods that detect copied regions without any modifications are not efficient. To deal with such problems there exist some approaches called CRM forgery detection in the literature.

(a) (b) (c)

Figure-2
An example of copy-rotate-move forgery: (a) the original image (b) the copy-move forged image, (c) the copy-rotate-move forged image[4]

One approach is applying Fourier-Mellin transform to the block[6]. However, according to their experimental results, the scheme performed well when the degree of rotation is small. Other approach suggested representing each block in log-polar coordinates[7]. Then they defined 1-D descriptor as summation of angle values to achieve rotational invariance. Since the method depends on the pixel values, it is sensitive to the change of the pixel values. To solve such problems There are some approaches that extracted interest points on the whole image by scale-invariant feature transform (SIFT). Such methods extract special points in images which are invariant against changes as scale modification or rotation. Furthermore use of special points instead of pixel blocks makes these methods less sensitive against degradations as noise or JPEG compression[8].

After extracting SIFT features the transform between two part of image containing such features are estimated. All parts of image are compared using their transform and by means of their similarities we make a map showing the probable regions with high likelihood to be duplicated from other regions[9].

As mentioned before these methods cannot detect the flat copied regions. This problem can be solved by using Zernik moments[5,9].

In this paper we propose a combinatory method to detect copied region of a forged image. At first we apply SIFT features and detect all copied region containing regions that were geometrically changed or rotated except flat copied region. Subsequently by applying Zernik moments based detection methods[5] we will detect flat copied region. The rest of this paper is organized as follows. SIFT feature based detection method is expressed in section II. In section III Zernik moments properties and Zernik moments based detection method is described and conclusion is presented in section IV.

Material and Methods

Duplication detection using SIFT features.

Assume that the original subset of pixel locations denotes with Ω_S and the corresponding duplicated region denote with Ω_T. The relation between the original and pasted region is $I(\Omega_T)=I(T_\theta(\Omega_S))$, where T_θ is the spatial transform of pixel locations between region Ω_S and Ω_T with parameter θ. The target is detecting Ω_S and Ω_T by means of spatial transform T_θ. in the case that the copied region is pasted without any transformation, T_θ is an identity.

To detect the potential duplication regions we first detect SIFT key points in the image and compute the SIFT features for them. Then we segment the whole image into none overlapping blocks and for each SIFT features in the blocks we compute its closest correspondence in the whole image.

By means of these matched SIFT key points we compute T_θ for scaling or rotations between the original and duplicated regions. Then by computing the correlations between these two regions we will achieve the final likelihood of two regions to be duplicated of each other. So this method steps are: (1) Computing SIFT features, (2) SIFT features matching and pruning, (3) estimating region transform and (5) detecting duplicated regions[8].

Now we will explain each of these steps. As explained in[10], for collecting SIFT features, at first we should identify key- pints which contain distinct image information and are invariant against scaling and rotations. Then at each key point a SIFT feature vector is generated from the Normalized histograms of local gradients in a neighborhood of pixels of that key point. The size of the neighborhood is determined by the scale of the key point, and all gradients are aligned with the dominant orientation at the key point. These steps ensure us that these descriptors are invariant to rotations and scaling. Normalizing the histogram to the unit length make SIFT features robust to contrast modifications[8]. According to [10], the final SIFT features are 128 dimensional vectors at each key point.

Matching and pruning SIFT key points: After collecting SIFT features, we should matches SIFT key points in each pixel blocks. Then for each SIFT key point in a block, we compute l_2 distances between its 128 dimensional SIFT features with key points not belong to the same pixel block, then we should find its nearest neighbor using the Best-Bin-First (BBF) algorithm[11]. The founded set of Matches of SIFT key point contains many mismatches. To remove these mismatches see[8].

Calculating region transform: After pruning we calculate the transform between original and copied region using ω_s and ω_T. For detecting copy move without any transformation, all pixels in the duplicated regions are related to the pixels in the original region with a common shift vector. According to this assumption, at first we compute the l_2 distances between each pair of matched SIFT key points. Key points corresponding to

translated regions have equal l_2, but in practice because of noise and other degradations, there will be a distribution of such distances. After that we will build a histogram of these distances and collecting key points pairs $P_s \subseteq \omega_s$ and $P_T \subseteq \omega_T$ with distances of maximum frequency of occurrence. The shift vector is then calculated as the difference between the means of P_S and P_T.

For detecting copy move with scaling, as in this case the l_2 distance between a pair of key points in the duplicated region is the multiple of that of their correspondence in the original region. In other words, for any two SIFT key points $(\vec{X},\vec{Y}) \in \omega_S$ and their correspondence $(\vec{X},\vec{Y}) \in \omega_T$, $\| \vec{X}-\vec{Y} \| / \| \vec{X}'-\vec{Y}' \|$ =const. However, due to imaging conditions and the matching procedure, there is a distribution of such scaling factors for a real image, which we estimate by computing pair wise l_2 distances for all SIFT key point pairs of ω_S and ω_T. We then form histograms of the ratios of such L_2 distance between corresponding pairs in ω_S and ω_T. The ratio with the maximum frequency is used as an estimation of the scale factor. Furthermore, key point pairs falling into that bin are used to estimate the translation between the original and the duplicated region as in the case of copy-move.
For detecting Copy move with rotation, we estimate the transform between two local coordinate systems of the original and duplicated region.

Two local coordinate systems of the original and the duplicated region. Specifically, we pick three non-collinear key points $(\vec{X},\vec{Y},\vec{Z}) \in \omega_S$ and their correspondences in $(\vec{X}',\vec{Y}',\vec{Z}') \in \omega_T$ that have the strongest matches (measured by the l_2 distances of their corresponding SIFT features). The two sets of vectors $(\vec{X}-\vec{Y},\vec{Z}-\vec{Y})$ form a local coordinate system for pixel locations in ω_S and ω_T respectively. Each pixel location can be written as a linear combination of the two vectors, with the two linear combination weights being the two coordinates. As rotation doesn't change these coordinates, we compute coordinates of each pixel location in ω_S for $(\vec{X}-\vec{Y},\vec{Z}-\vec{Y})$. Their transformed correspondences are obtained by using the same set of coordinates in the coordinate system given by $(\vec{X}'-\vec{Y}',\vec{Z}'-\vec{Y}')$. After adjusting the rotation, translation between regions is estimated as the shift between the means of the two set of SIFT key points[8].

Zernik moments properties: Zernik moments [14] are rotation invariant and robust to noise, so if we use a descriptor based in these moments, it will inherit this characteristics. In (ρ,θ) polar coordinates, the Zernike radial polynomials $R_{mn}(\rho)$ are defined [15] as:

$$R_{nm}(\rho)=\sum_{s=0}^{(n-|m|)/2}(-1)^s \frac{(n-s)!}{s!((n+|m|)/2-s)!(n-|m|)/2-s)!}\rho^{n-2s} \qquad (1)$$

where n is a non-negative integer, and m is a non-zero integer subject to the following constraints: $n-|m|$ is even and $|m| \le n$. The (n, m) order of the Zernike basis function, $V_{nm}(\rho,\theta)$ defined over the unit disk is

$$V_{nm}(\rho,\theta) = R_{nm}(\rho)\exp(jm\theta).\rho \le 1 \qquad (2)$$

The Zernike moment of an image is defined as

$$Z_{nm} = \frac{n+1}{\Pi}\iint_{unitdisk} V_{nm}^{*}(\rho,\theta) f(\rho,\theta) \qquad (3)$$

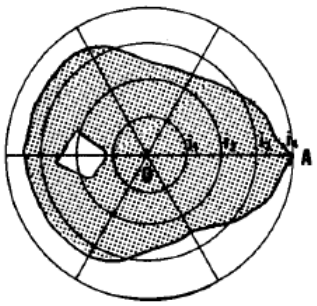
Where V_{nm}^{*} is a complex conjugate of V_{nm}.

The extraction of the Zernike moment descriptor from an image is done this way: First, the input image is binarized. Since the Zernike moments are defined over a unit disk, the radius R of a circle is determined to enclose the shape completely, from the centroid of the binarized shape in the image to the outer most pixel of the shape. The shape is then re-sampled to normalize to the size of $2R \times 2R$ pixels. This normalization step allows the scale invariance for the descriptor. Thirty-six Zernike moments of order from zero to ten for both n and m are then extracted from the normalized image, and the magnitudes are used as the descriptor.

Zernike moments have the following properties: They are rotation invariant, robust to noise, have no redundancy in the information they provide (because the bases are orthogonal), effective in a way that they describe better an image than any other type of moments, and they order multi-level representation. Although they have interesting characteristics, their calculation has several problems: the image coordinate space must be transformed to the domain where the orthogonal polynomial is defined (unit circle for the Zernike polynomial), the continuous integrals used to compute them have to be approximated by discrete summations (which leads to numerical errors and affects the rotation invariance) and they are costly to compute as their order is increased. Matlab code can be found at. Zernike Moments are also used as a part of more complex descriptors, as it can be seen in[17]. Descriptor: The Feature Vector will consist of the coefficients of the Zernike moments.

Shape Matrix: It is similar to the Grid-based preprocessing procedure that was explained in the Feature Detection chapter (and that will in the Grid-based Descriptor that will be presented later) with the difference of using a series of concentric circles and radial lines instead of rectangular grids.

In this method[18] a shape is transformed into a matrix by polar quantization of the shape. This method can be better understood by looking at figure-3.



	0	1	2	3	4
0	1	1	1	1	1
1	1	1	1	0	0
2	1	1	1	1	0
3	1	1	0	1	0
4	1	1	1	1	0
5	1	1	1	0	0

(a) **(b)**

Figure-3
(a) A shape and (b) I ts shape matrix [18]

(a) (b) (c) (d)

Figure-4
Examples of CRM forgery and its detection result: (a) the forged image by CRM forgery of 10, (b) forged region, (c) detected region, and (d) (forged region ∩ detected region)[4]

If we consider the centre of gravity of the shape O and we keep the maximum radius of the shape $\overline{OA}$ with length L, in order to obtain an $m \times n$ size matrix representation of the shape, we divide $\overline{OA}$ into n-1 equal distances and draw circles centred in O and radii L/(n-1),2L/(n-1),...(n-1)L/(n-1). If the circles intersect in the maximum radius of the shape, each circle is divided into m equal arcs, each arc being $360/m$ degrees.

To construct the Shape Matrix the next algorithm is used: i. Create an $m \times n$ matrix that will be called M, ii. From i = 0 to n-1 and from j = 0 to m-1, if the point with polar coordinates $(il/(n-1),(360/m))$ lies inside the shape, then M(i,j) = 1 otherwise let M(i,j) = 0.

When implementing the Shape Matrix information is gathered in an object centred coordinate system that is normalized with respect to the maximum radius of the shape. The obtained Shape Matrix (and its related descriptor) is translation, rotation and scale invariant.

According to Zernike moment properties it is clear that these features are efficient for flat regions, in this paper we apply SIFT feature method and subsequently Zernike moment method to detect duplicated regions even if they rotated or scaled before pasting and even if the region is flat.

Results and Discussion

To implement the proposed method, we first detect SIFT key points in the image and compute the SIFT features for them. Since in flat regions there is no SIFT keypoint, for such regions we find Zernik moment. We will describe how to find copied regions whit SIFT features and Zernikmoments.

Showing copied regions whit SIFT keypoints: After estimating region transform, we can found the correspondence between pixels in original and duplicated region. Using this correspondence, we create a map of region correlations to identify the original and duplicated regions.

To achieve this target, we segment the whole image into overlapping contour blocks. By calculated transform we compute the correlation coefficient between each contour block and its correspondence and generate the correlation map. Then we transform the correlation map to binary form. Then by deleting the regions with areas smaller than a pre given threshold, we reduce the effect of noise.

At last the contours of the potentials and original regions are connected with mathematical morphological operations[12]. After applying SIFT features we can detect the duplicated regions even they are scaled or rotated before pasting. As mentioned before SIFT features cannot detect the flat copied regions. Zernik Moments overcome this problem.

$$B_{ij}(x,y)=f(x+i,y+j) \quad (4)$$

Where

$$x,y\in\{0,...,L-1\},i\in\{0,...,M-1\},and$$
$$j\in\{0,...,N-1\} \quad (5)$$

Hence, we are able to obtain N of overlapped sub-blocks from the suspicious image.

$$N_{block}=(M-L+1)\times(N-L+1) \quad (6)$$

We assume that the pre-defined size of block is smaller than the tampered region. After that, the Zernike moments of particular degree n are calculated from each block and vectorized by getZernikeMoments function as follows:

$$V_{ij}=getZernikeMoments(B_{ij},n), \quad (7)$$

Where function V=getZernikeMoments (Block,nMax)

Where function V=getZernikeMoments (Block,nMax)

i. Vector **V**
ii. **for** *n*=0 to n Max **do**
iii. **for** m=0 to n **do**
iv. if (n-m)%2=0 **then**
v. **V.***pushback* $(\frac{n+1}{\pi}\sum\sum(Block\times V_{nm}^{*}))$
vi. **end if**
vii. **end for**
viii. **end for**
ix. **return V**

By analyzing getZernikeMoments function of given order nMax, the entire number of moment is

$$N_{moments}=\sum_{i=0}^{nMax}(\left\lfloor\frac{i}{2}\right\rfloor+1) \quad (8)$$

After that, we can construct Z, a set of vectorized moments V_{ij}.

$$\begin{bmatrix} V_{00} \\ ... \\ V_{(M-L)(N-L)} \end{bmatrix}$$

The set Z is then lexicographically sorted since each element of Z is a vector. The sorted set is denoted as $\hat{z}$. From the set $\hat{z}$, the Euclidean distance between two adjacent pairs of $\hat{z}$ is calculated. If the distance is smaller than the pre-defined threshold D1 we consider the inquired blocks as a pair of candidates for the forgery:

$$\hat{Z}_p=(\hat{z}_1^{\,p},\hat{z}_2^{\,p},...,\hat{z}_{Nmoments-1}^{\,p},\hat{z}_{Nmoments}^{\,p}),$$
$$\hat{Z}_{p+1}=(\hat{z}_1^{\,p+1},\hat{z}_2^{\,p+1},...,\hat{z}_{Nmoments-1}^{\,p+1},\hat{z}_{Nmoments}^{\,p+1}), \quad (9)$$
$$\sqrt{\sum_{q=1}^{Nmoments}(z_q^{p}-z_q^{p+1})}$$

Due to the fact that the neighboring blocks might result in relatively similar Zernike moments, we calculate the distance between the actual blocks of the image as follows:

$$\sqrt{(i-k)^2+(j-1)^2}$$
$$\hat{Z}_p=V_{ij}\,and\,\hat{Z}_{p+1}=V_{kl} \quad (10)$$

We determine whether the investigated blocks are duplicated or not according to the equation 9 and equation 10.

You can see related results in figure-5.

Figure-5
Related result

Conclusion

Since the use of the internet and digital images in it has been grown, these images are used as information sources. Moreover, nowadays in courts digital images can present as testimony. There are some approaches to detect duplicated regions either the copied part is pasted in the other region without any modifications or with modifications such as rotation or scaling. SIFT features are invariant against rotation and scale changing but failed to detect flat copied regions.

Zernik moments are invariant against rotations and degradations such as additive white Gaussian noise, JPEG compression and blurring and it is efficient for flat regions but failed for scale changing. In this paper we propose a combinatory method to detect copy-move forgery.

Composing these two methods will increase the precision and robustness, but if we apply these two feature extraction methods on the overall image, the proceeding time will increase. To address this problem, at first we apply SIFT feature extraction method to find SIFT key point on the image, as there is no SIFT key points in flat region of image, and Zernik moments are good for flat regions, for such regions we will apply Zernik moment feature extraction method to extract zernik moments.

Consequently copy-pasted regions in overall image even in flat regions will detect while the proceeding time is efficient.

References

1. Sharma Kalpa, Health IT in Indian Healthcare System: A New Initiative, *Res. J. Recent Sci*., **1(6)**, 83-86 **(2012)**

2. Shahaboddin Shamshirband and Ali Za'fari., Evaluation of the Performance of Intelligent Spray Networks Based On Fuzzy Logic, *Res. J. Recent Sci*., **1(8),** 77-81 **(2012)**

3. Bora Abhijit, Science Communication through Mass Media, *Res. J. Recent Sci*., **1(1)**, 10-15 **(2012)**

4. M. Stamp and P. Stavroulakis, *Handbook of Information and Communication Security* **(2010)**

5. S. Jin Ryu, M. Jeong Lee, and H. Kyu Lee, Detection of copy-rotate- move forgery using Zernik moments **(2010)**

6. Bayram S., Sencar H.T. and Memon N., An efficient and robust method for detecting copy-move forgery, *Proc. of ICASSP*, **(2009)**

7. Solorio B., Nandi S. and A.K., Passive method for detecting duplicated regions affected by reflection, rotation and scaling, *EUSIPCO*, **(2009)**

8. Pan X. and Lyu S., Detection image region duplication using SIFT features **(2008)**

9. Bernal J., Vilarino F. and Sanchez J., Feature detectors and descriptor: where we are now, september **(2010)**

10. Lowe D., Distinctive image features from scale-invariant keypoints, *IJCV*, **60(2)**, 91–110 **(2004)**

11. Beis J. and Lowe D., Shape indexing using approximate nearestneighbour search in high-dimensional spaces, *CVPR*, **(1997)**

12. Suzuki S. and Abe K., Topological structural analysis of digital binary images by border following, *CVGIP*, **30(1)**, 32–46 **(1985)**

13. Popescu A.C. and Farid H., Exposing digital forgeries by detecting duplicated image regions, *Technical Report TR2004-515, Department of Computer Science, Dartmouth College*, **(2004)**

14. Khotanzad A. and Hong Y.H., Invariant image recognition by Zernike moments, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 489 {497, 1990. [Online]. Available: http://tinyurl.com/33jrzzq

15. Kim W.Y. and Kim Y.S. A region-based shape descriptor using Zernike moments, *Signal Processing: Image Communication*, **16(1-2)**, 95-102, **(2000)** [Online]. Available: http://tinyurl.com/2935dvy

16. Wolf C., Zernike moments matlab code, *Universit_e de Lyon, INSA de Lyon, France*. [Online]. Available: http://tinyurl.com/39s9lwc

17. Hwang S., Billinghurst M. and Kim W. Local Descriptor by Zernike Moments for Real-time Keypoint Matching, *in 2008 International Congress on Image and Signal Processing,* **(2008)** [Online]. Available:http://tinyurl.com/326dncn

18. Zhang D. and Lim M.C.Y., An e_cient and robust technique for region based shape representation and retrieval, in *6th IEEE/ACIS International Conference on Computer and Information Science*, **2007,** ICIS 2007, 2007, pp. 801{806. [Online]. Available: http://tinyurl.com/37ktsvs

19. Goshtasby A., Description and Discrimination of Planar Shapes Using Shape Matrices, *Proc. IEEE,* **67**, 786-804 **(1979)** [Online]. Available: http://tinyurl.com/35lqkv8

20. Irene Amerini, Lamberto Ballan, Student Member, IEEE, Roberto Caldelli, Member, IEEE, Alberto Del Bimbo, Member, IEEE, and Giuseppe Serra., A SIFT-based forensic method for copy-move attack detection and transformation recovery, *IEEE* **(2011)**