Detection of Region Duplication Forgery in Digital Images Using SURF

B.L.Shivakumar[1] and Lt. Dr. S.Santhosh Baboo[2]

**[1]Department of Computer Applications, SNR Sons College
Coimbatore – 641 006 , Tamilnadu, India**

**[2]PG & Research Dept. of Computer Applications, D.G. Vaishnav College
Chennai - 600 106, Tamilnadu, India**

Abstract

An Image would yield better impact in convincing someone of something rather than pure description by words. Digital images are widely used in various fields like medical imaging, journalism, scientific manipulations and digital forensics. However, images are not reliable as it may be. Digital images can be easily tampered with image editing tools. One of the major problems in image forensics is determining if a particular image is authentic or not. Digital image forensic is an emerging field of image processing area. Copy-move forgery is one type of image forgery in digital image forensic where various methods have been proposed in the field to detect the forgery. In this paper a technique is presented to detect Copy-Move Forgery based on SURF and KD-Tree for multidimensional data matching. We demonstrate our method with high resolution images affected by copy-move forgery.

Keywords: *Image forensic, Copy-move forgery, SURF, KD-tree*

1. Introduction

Nowadays, digital images are widely used in our society. From newspapers to the tabloid magazines, scientific journals, physicians in medical field, fashion industries, court rooms and other outlets heavily depend on digital images. Information integrity is fundamental in many fields. Historically we had confidence in the integrity of imagery; today's digital technology has begun to erode this trust. Even though tampering with photograph is not new, during the past few years, doctored images are appearing with growing frequency and sophistication. This is mainly due to the availability of low-cost hardware and photo editing software which makes it easy to manipulate and alter digital images without leaving any obvious trace. For an example recently, (September 2010) Egypt's state-run newspaper, *Al-Ahram,* published the altered photo (Fig. 1) of Egyptian President Mubarak walking with Israeli, US, Palestinian and Jordanian leaders during the latest Middle East peace talk

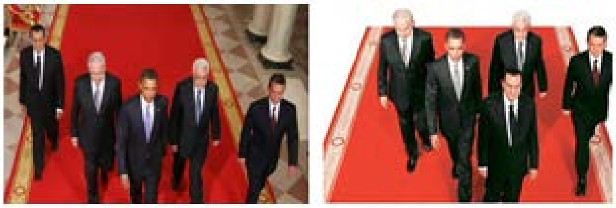

(a) Original photo (b) Altered photo

Fig 1: (a) Original photo shows President Mubarak is walking behind the other leaders (b) Altered photo shows President Mubarak leading the group.

With the emergence of digital forensics over the past few years, trust in the field of digital imagery has been restored. Forgery detection aims to tell whether the digital image content is authentic without image forgery operations. Till now, several methods have been proposed to detect forgeries. Basically, the digital image forgery detection methods are classified into Active Digital Image Forensics and Passive Digital Image Forensics or Blind Digital Image Forensics [1]. Unlike the active method such as digital watermarking and digital signature (Fig. 2(a)), the passive approach does not rely on pre-embedded information (Fig. 2(b)).

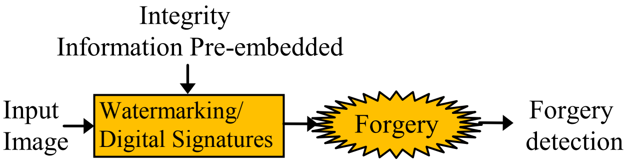


Fig. 2(a): Active forgery detection scheme

Input Image
Forgery
F orgery detection

Fig. 2(b): Passive forgery detection scheme

Over the past five years have seen a growth on passive digital image tampering detection, which could be categorized at three levels [2]:

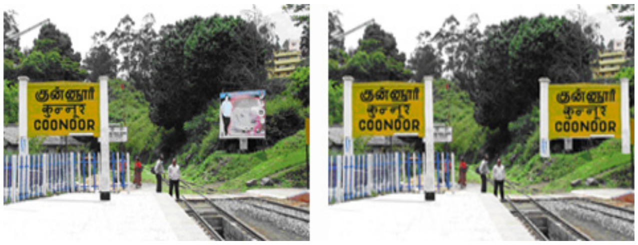
1) **Low Level:** Statistical characteristics of digital image pixels or DCT coefficients are used to detect the tampering.

2) **Middle Level:** Methods at this level use simple semantic information to detect the trace of tampering

3) **High Level** i.e., semantic level: Sometimes tampering is done with an intention to change the meaning of image content it originally conveyed, which becomes very difficult for computer to use semantic information to detect forgery. For example, it does not make sense to have an image in which Barrack Obama shaking hands with Osama Bin Laden.

1.1 Copy-Move Forgery

Copy-move forgery, as depicted in Fig. 3, is one type of forgery, in which one part of the image itself is copied and pasted into another part of the same image to conceal a person or an object in the scene.



(a) (b)

Fig 3: An example of image forgery. (a) the original image with one name board on the left side of the railway track. (b) forged image with two name boards.

Since, the copied part come from the same image in copy-move forgery, the colour palette, noise components, lighting, and most other properties will be compatible with the rest of the image; it becomes harder for human eye to detect. On the basis of our preliminary study [3] a methodology based on SURF is proposed to detect copy move forgery in digital images with high resolution. Large images are considered in our work because there is an overall higher number of feature vectors, and thus there is considerably a higher chance of matching wrong blocks. The proposed method has also been tested against rotation in selected angle, scaling and images distorted by adding a Gaussian noise.

The rest of the paper is structured as follows: Section 2 presents related work regarding copy-move forgery detection and it reviews the SURF technique in Section 3. Section 4 presents the proposed method with experimental results on forgery detection in Section 5 and conclusion is finally drawn in Section 6.

2. Review of Literature

During the past five years several researchers have developed different techniques to detect copy-move forgery. The copy-move forgery introduces a correlation between the original image region and the pasted region. This form of forgery could be detected by direct method by exhaustive search [4]. This approach is simple and effective for small-sized image and computationally complex and even impractical for image of bigger size. To make the computation quicker, Fridrich et. al [5] proposed an approach in which the image is segmented into overlapping small blocks and lexicographically sorted the image blocks to check whether adjacent blocks are similar or not. To reduce dimension DCT block representation, A.C. Popescu et . al. [6] applied PCA (Principle Component Analysis) and the detection consumed less time. G .Li.et. al. [7] introduced a sorted neighbourhood approach based on DWT (Discrete Wavelet Transformation) and SVD (singular Value Decomposition). These algorithms based on block-matching and are computationally complex. Some algorithms are weak to locate the copy-move region after-copying manipulations, such as lossy compression, blurring or combination of these operations.

E.S.Gopi et. al [8] proposed a method to identify the region of digital forgery in uncompressed TIFF images, GIF and JPEG images with minimal compression by exploiting property of correlation by using Auto Regessive coefficients and Artificial Neural Network(ANN). Recently, Seung_Jin Ryu et. al [9] proposed a method using Zernike moments, which was weak against scaling and other type tampering based on affine transform. Hwei-Jen Lin et. al.[10], applied radix sort to improve the time complexity. Their method does not deal with rotation in arbitrary angles. B.Mahdian et. al. [11] proposed an approach based on blur moments invariants which has a problem with uniform areas in the image. Scale Invariant Features Transform (SIFT), which is invariant to illumination, scaling, rotation etc was applied by H.Huang et. al [12] to detect duplication region.

Recently, Xu Bo. et. at. [13] proposed a method to identify duplication region using SURF. In their approach the keypoints matching is done by matching between two subsets of the keypoints set of the test images. As shown in Fig. 4 the operations performed on the images are small region of copy area.

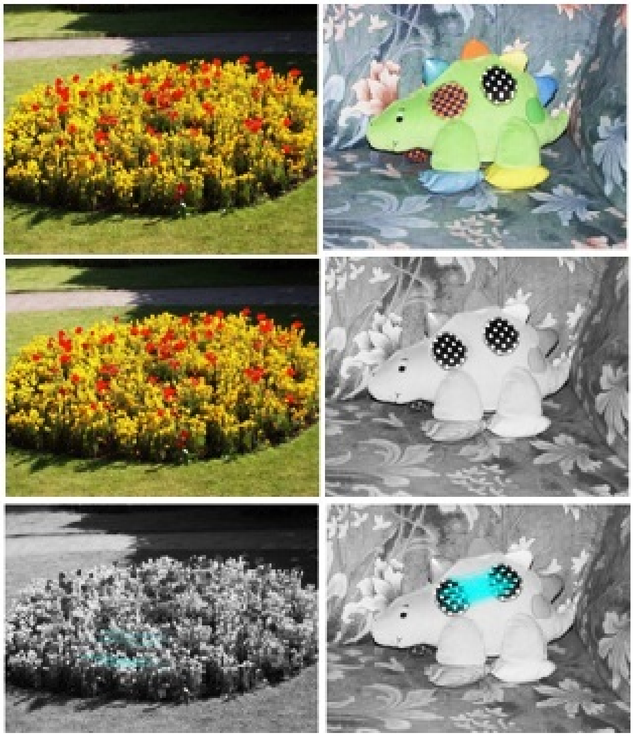


Fig 4. Test images used by Xu Bo et. at. in their experiments with small size of copied area. Top row shows the original images and the tampered images in the middle row followed by the output images in the last row with copied and pasted regions highlighted in blue colour.

3. Review of SURF algorithm

The task of finding point correspondence between two images of an object or same scene is part of many computer vision applications. Recently Herbert Bay et. al. proposed fast detectors and descriptors, called SURF (Speeded Up Robust Features) [14]. SURF's detector and descriptor is said to be faster and at same time robust to noise, detection displacements and geometric and photometric deformations.

A wide variety of detectors and descriptors such as SIFT, PCA-SIFT, GLOH have been proposed in the literature. Also, detailed comparisons and evaluation on detectors and descriptors have been performed [15,16]. SURF is claimed to be comparable to or even better than other detectors and descriptors [17]. SURF is explained in the following section.

3.1 Pre-processing

Normally, interest points which are detected under illumination change in an image. Therefore, the first step is to convert the colour image into a g ray scale image. Moreover, gray scale image are simple to enhance and interpret.

3.2 Interest point detection

After the image is transformed into gray scale, the next task is to localise the interest points. The SURF detector is based on integral image and Hessian matrix approximation.

3.2.1 Integral image

The performance of SURF algorithm is much attributed to the use of an intermediate image representation known as the "Integral Image". The integral image, denoted $ii(x,y)$ at a point (x,y) for an input image $i(x,y)$, is calculated by the sum of the values between the point and origin(Fig. 6(a)). Formally integral image could be defined by the formula

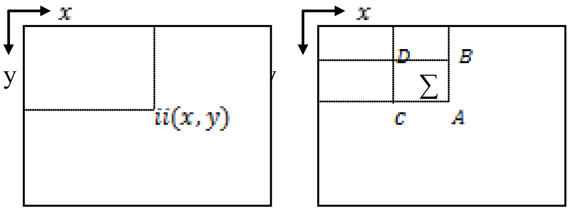
$$ii(x,y) = \sum_{\substack{x' \le x \\ y' \le y}} i(x',y'), \qquad (1)$$

The integral image can be computed recursively by using the following pair of recurrences:

$$s(x,y) = s(x,y-1) + i(x,y) \qquad (2)$$

$$ii(x,y) = ii(x-1,y) + s(x,y) \qquad (3)$$

Using integral image, it ta kes three additions and four memory access to calculate the sum of the intensities over any upright, rectangular area. The sum of pixel intensities, for a rectangle bounded by vertices A, B, C and D (Fig. 5(b)) is calculated by $\sum = A + D - (C + B)$



(a) (b)

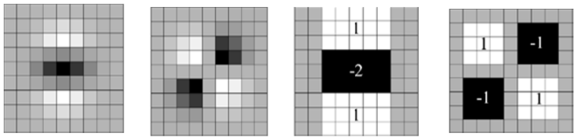
3.2.2. Hessian matrix-based interest point

The SURF feature detector is based on the Hessian matrix because of its good performance in accuracy. The Hessian matrix is defined as H(x, σ) for a given point $\boldsymbol{x} = (x, y)$ in an image as follows:

$$H(x,\sigma) = \begin{bmatrix} L_{xx}(x,\sigma) L_{xy}(x,\sigma) \\ L_{xy}(x,\sigma) L_{yy}(x,\sigma) \end{bmatrix} \qquad (4)$$

where L_{xx} *(x,σ)* is the convolution of the Gaussian second order derivative $\frac{\partial^2}{\partial x^2} g(\sigma)$with the image I in point x and similarly for L_{xy} *(x,σ)* and L_{yy} *(x,σ)*. These derivatives are called as Laplacian of Gaussians.

Working from this the determinant of the Hessian for each pixel in the image is calculated and the values are used to find interest point. SURF approximates Gaussian second order derivatives with box filters. These approximate Gaussian second order derivates can be evaluated at very low computational cost by using the integral image. The box filter masks with different sizes are used to convolve all intensity values at different scale layers in the integral image. The Difference of Gaussians (DoG) approximations are obtained by subtracting the filtered image from each other. The SURF uses 9 x 9 box filters (Fig. 6(a) and 6(b)) as the initial scale layer which is equivalent to Gaussian derivates with σ =1.2 and represent the lowest scale for computing the blob response maps and denoted as D_{xx}, D_{yy} and D_{xy}. The second order Gaussian partial derivatives with the box filters in $y-$ direction and xy $-$direction are shown in Fig 7 (a) and 7(b) respectively.



(a) (b)

Fig 7: (a) Left: Gaussian second order partial derivatives in y-direction (b) Left: Gaussian second order partial derivatives in *xy*-direction Right: Approximation of using box filter Right: Approximation of using box filter

The following formula is used in SURF for an accurate approximation for the Hessian determinant.

$$\det(H_{\text{approx}}) = D_{xx}\, D_{yy} - (0.9D_{xy})^2 \qquad (5)$$

where $w \approx 0.9$, which assures energy conservation of the approximation.

After the approximation of the DoG is determined, the next process is to construct functions that can be used to select extrema points.

3.2.3. *Interest point Descriptors*

The SURF descriptor is extracted from an image in two steps : the first step is assigning an orientation based on the information of a circular region around the detected interest points. The orientation is computed using Haar-wavelet responses in both x and y direction. Once the Haar-wavelet responses are computed, they are weighted with a Gaussian with σ = 2.5s centered at the interest points. In a next step the dominant orientation is estimated by summing the horizontal and vertical wavelet responses within a rotating wedge which covering an angle of π/3 in the wavelet response space. The resulting maximum is then chosen to describe the orientation of the interest point descriptor.

In a second step, the region is split up regularly into smaller square sub-regions and a few simple features at regularly spaced sample points are computed for each sub-region. The horizontal and vertical wavelet responses are summed up over each sub-region to form a first set of entries to the feature vector. The responses of the Haar-wavelets are weighted with a Gaussian centered at the interest point in order to increase robustness to geometric deformations and the wavelet responses in horizontal d_x and vertical Directions d_y are summed up over each sub-region. Furthermore, the absolute values $|d_y|$ and $|d_y|$are summed in order to obtain information about the polarity of the image intensity changes. Therefore each sub-region has a four-dimensional descriptor vector

$$V = (\sum d_x, \sum|d_x|, \sum|d_y|) \qquad (6)$$

where dx denotes the horizontal wavelet response and dy the vertical response.

4. Proposed method

The proposed system is based on SURF algorithm to extract features along with KD-tree is used to identify the duplicated region. In copy-move forgery the copied part has basically the same appearance of the original one; therefore, keypoints extracted in the forged region will be quite similar to original ones. The matching among SURF features can be adopted for the task of determining possible tampering. A simple schematization of the proposed system is shown is Fig. 4. The first step consists of SURF feature extraction. The second step is devoted to keypoint matching followed by verification step filters matching pair that follows a common pattern.

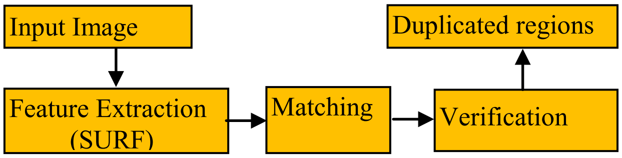


Fig 4. Overview of the proposed system

4.1 Descriptors matching

In our system to identify the duplication region the KD-tree [18] algorithm is used for key points matching. In most of the copy-move forgery detection algorithms, lexicographic sorting are used, which is said to be too sensitive to the transformations and yields a lower false positive rate compared to KD-Tree which produces reliable results and a lower false negative rates.[19] The KD-tree is commonly used structure for searching for nearest neighbours. The KD tree pre-processes data into a data structure allowing us to make efficient range queries. It is a binary tree that stores points of a k-dimensional space in the leaves. In each interval point, the tree divides the k-dimensional space into two parts with (k-1) dimensional hyper plane. Suppose a KD-tree consists of N feature vectors, it requires $O(N \log_2 N)$ operations to be constructed and $O(\log_2 N)$ to be searched.

Given a test image, a set of keypoints $\mathbf{X} = \{ x_1, ..., x_n \}$ with their corresponding SURF descriptors $\{f_1, ..., f_n\}$ is extracted. A matching operation is performed in the SURF space among $\mathbf{f_i}$ vectors of each keypoint to identify similar local patches in the test image. The best candidate match for each keypoint $\mathbf{x_i}$ is found by identifying its nearest neighbour from all the keypoint with minimum Euclidean distance in SURF space. The KD-tree is used for searching nearest neighbours with a threshold T_h .

5. The Experimental Results

The proposed method has been implemented using Matlab 7.6 a computer of CPU 2.20 GHz with memory of 3 GB. The SURF algorithm is used to detect the key points and get the descriptors. In the experiment the extended descriptor mode is used to get the 128-d SURF descriptors and KD-tree algorithm is used for key points matching. The images have been selected from the dataset proposed by Christlein. et. at.[19]. Large images which have a relatively high resolution of more than 3000 x 2400 pixels are considered for our test since an overall higher number of feature vectors exits, and thus there is a considerably higher probability of matching wrong block. The duplicated regions in the tampered image also significantly vary in size and texture.

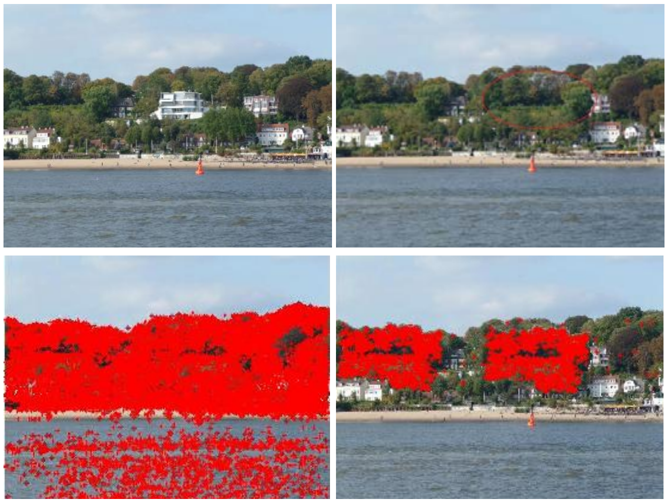


Fig 8. The original image *Beachwood* (upper left) is shown in the in the top row.. The *Beachwood* (3264 x 2448 pixels) is forged with green patch to conceal a building is shown in the (upper right) in the top row. The forged image after extracting SURF keypoints (bottom left) in the second row. The detction result is shown in (bottom right) in the second row.

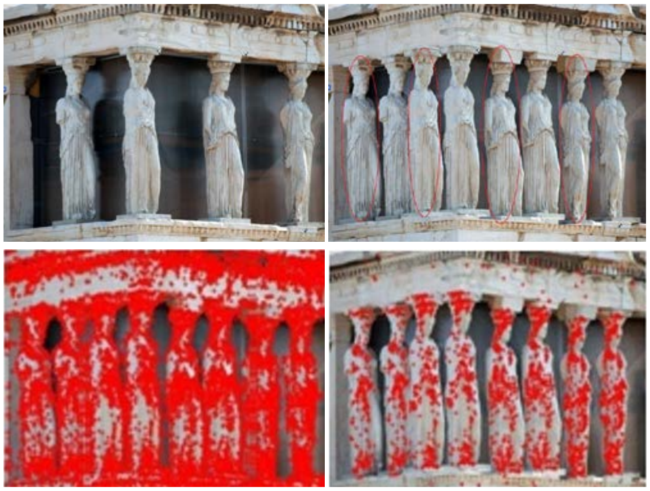


Fig.9. The test image *Acropolis* (3872 x 2592 pixels) has many copied regions with different size which is marked with ellipse.The original image is shown in the (upper left) in the top row. The tampered image is shown in the (upper right) in the top row. The forged image after extracting SURF keypoints (bottom left) in the second row. The detection result is shown in (bottom right) in the second row.

The proposed detection method detects the duplication region after SURF keypoints which are extracted from the images, and their descriptors are matched with a threshold T_h (often fixed as 0.045). We found that when the threshold was increased there were more m atch points which also resulted in more false match points. It is interesting to note that the number of false matches are higher for *Acropolis* compared to B*eachwood* for the same threshold value beacuse the image resolution of *Acropolis* is higher than the *Beachwood*.

The proposed methodology has also been tested in terms of detection performance from robustness point of view; in particular, the impact of rotation, scaling and noise addition on *Beachwood* has been investigated. More detected results over tampered images with post processing rotation; scaling and noise are shown in Figs. 10 – 12.

To deal with rotation, we considered rotations through different angles. Fig 10 shows the comparsion between the rotation angle 30 degree clockwise and 30 degree anticlockwise of the tampered region.

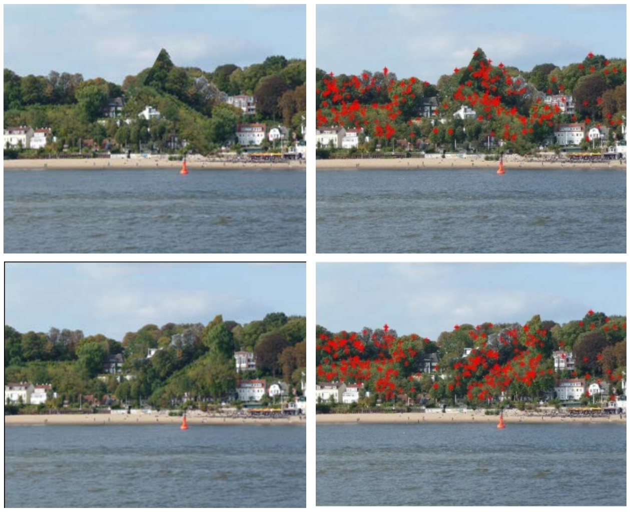
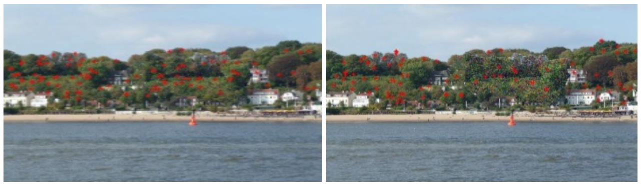


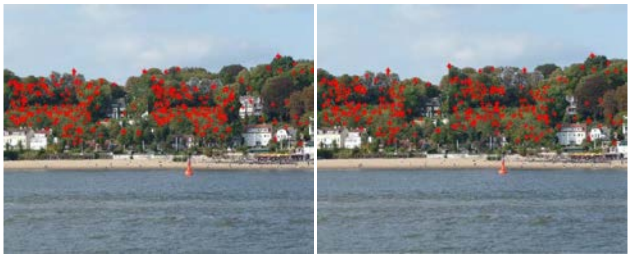
Fig 10. Copied region rotated in angle 30 degree clockwise (upper left) and the detected result (upper right) and the tampered region is rotated 30 degree anticlockwise (bottom left) and the detected result (bottom right).

The proposed methodology has also been tested on images that are distorted by adding Gaussian noise to the duplicated region and detected result are shown in Fig. 11



(a) (b)

Fig. 11. Detected result with Gaussian Noise
(a) SNR=10db (b) SNR=20db.



(a) (b)

Fig 12. Detected results for the tampered image *Beachwood* with scaling factor. (a) scaling with 90% (b) scaling with 115%.

The experimental results also show that the proposed system reliably detects tampered region post processing with sufficient number of matched keypoints. However, the number of matched keypoint is comparatively less for a threshold T_h, after different attacks such as rotation, scaling and noise applied to the image with copy-move forgery.

6. Conclusion and Future Work

We have proposed an automatic and robust copy-move forgery detection method based on SURF, which detects duplication region with different size. Experimental result shows that the proposed method can detect copy-move forgery with minimum false match for images with high resolution. However, a few small copied regions were not successfully detected. As part of our future work, we will continue to examine copy-move forgery to identify tampered region boundary and reduce the false match rate.

References

[1] B.L.Shivakumar and S.Santhosh Baboo, “Digital Image Forgery Detection”, *SAJOSPS*, Vol. 10(2), pp. 116-119, 2010

[2] Wei Wang, Jing Dong, and Tieniu Tan, “A Survey of Passive Image Tampering Detection”, pp 308-322, 2009

[3] B.L.Shivakumar and S.Santhosh Baboo, “Detecting Copy-Move Forgery in Digital Images:A Survey and Analysis of Current Methods”, *GJCST*, Vol 10(7) (2010).

[4] A.N. Myna, M. G. Venkateshmurthy, and C. G. Patil, “Detection of Region Duplication Forgery in Digital Images Using Wavelets and Log-Polar Mapping,” in Proceedings of the International Conference on C omputational Intelligence and Multimedia Applications (ICCIMA 2007), Vol. 3, pp. 371-377, 2007.

[5] Fridrich, D. Soukal, and J. Lukás, "Detection of copy move forgery in digital images," in Proc. Digital Forensic Research Workshop, Aug. 2003

[6] A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Traces of Resampling," *IEEE Transactions on Signal Processing*, Vol. 53,2005, pp. 758-767.

[7] G. Li, Q. Wu, D. Tu, and S. Sun, "A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries based on DWT and SVD," in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing China, July 2-5, 2007, pp. 1750-1753.

[8] E. S. Gopi, N. Lakshmanan, T. Gokul, S. KumaraGanesh, and P. R. Shah, "DigitalImage Forgery Detection using Artificial Neural Network and Auto Regressive Coefficients," Electrical and Computer Engineering, 2006, pp.194-197.

[9] Seung-Jin Ryu, Min-Jeong Lee and Heung-Kyu Lee, "Detection of Copy-Rotate-Move Forgery using Zernike Moments", in: 12th International Workshop on Information Hiding, Calgary, Alberta, Candada, 2010

[10] Hwei-Jen Lin, Chun-Wei Wang, Yang-Ta Kao, "Fast Copy-Move Forgery Detection", in WSEAS Transaction on Signal Processing, Vol 5(5), pp. 188-197, May 2009.

[11] B. Mahdian and S. Saic, "Detection of Copy-Move Forgery using a Method Based on Blur Moment Invariants," Forensic Science International, vol. 171, no. 2, pp. 180–189, Dec. 2007.

[12] 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, pp. 272-276, 2008.

[13] Xu Bo,Wang Junwen, Liu Guangjie, Dai Yuewei, "Image Copy-Move Forgery Detection Based on SURF", in Proceedings of the International Conference on Multimedia Information Networking and Security (MINES) pp. 889 - 892, 2010

[14] Herbert Bay, Andreas Ess, Tinne Tuytelaars, and Luc Van Gool. Surf: Speeded up robust features. Computer Vision and Image Understanding (CVIU), 110(3):346–359,2008

[15] Krystian Mikolajczyk and Cordelia Schmid. A performance evaluation of local descriptors. IEEE Transactions on Pattern Analysis and Machine Intelligence, 27(10): 1615–1630, 2005.

[16] Bauer, J., Sunderhauf, N., & Protzel, P., Comparing Several Implementations of Two Recently Published Feature Detectors. In Proc. of the International Conference on Intelligent and Autonomous Systems, IAV, Toulouse, France, 2007.

[17] Luo Juan, Oubong Gwun, A Comparison of SIFT, PCA-SIFT and SURF, *IJIP*, Vol. 3(4), 2009

[18] A.Moore. An introductory tutorial on KD-trees. Technical Report No. 209, University of Cambridge, 1991.

[19] V. Christlein, C. Riess, and E. Angelopoulou, "A Study on Features for the Detection of Copy-Move orgeries," in GI SICHERHEIT, 2010.

B.L.Shivakumar received his B.Sc (Computer Science) from Bharathiar University, Coimbatore and Master degree in Computer Science from Bharathidasan University, Thiruchirappalli in 1994 and 1996 respectively. He received M.Phil degree in Computer Science from Manonmaniam Sundaranar University, Tirunelveli in 2003. He also received Post Graduate Diplomas in Business Administration (PGDBA), Co-operative Management (PGDCM) and Bachelor degree in Library and Information Science (BLIS) from Annamalai University, Chidambaram. He is pursuing his Ph.D at School of Computer Science and Engineering, Bharathiar University, Coimbatore. He is currently working as Head in the Department of Computer Applications, SNR Sons College, Coimbatore. He has 15 years of teaching experience. He has presented many papers in various national and international conferences and published articles in research journals. His research interests are Computer Vision, Image processing and Cloud Computing.

Lt. Dr.S.Santhosh Baboo has around twenty years of postgraduate teaching experience in Computer Science, which includes Six years of administrative experience. He is a member, board of studies, in several autonomous colleges, and designs the curriculum of undergraduate and postgraduate programmes. He is a consultant for starting new courses, setting up computer labs, and recruiting lecturers for many colleges. Equipped with a Masters degree in Computer Science and a Doctorate in Computer Science, he is a visiting faculty to IT companies. It is customary to see him at several national/international conferences and training programmes, both as a participant and as a resource person. He has been keenly involved in organizing training programmes for students and faculty members. His good rapport with the IT companies has been instrumental in on/off campus interviews, and has helped the post graduate students to get real time projects. He has also guided many such live projects. Lt.Dr. Santhosh Baboo has authored a commendable number of research papers in international/national Conference/journals and also guides research scholars in Computer Science. Currently he is Reader in the Postgraduate and Research department of Computer Science at Dwaraka Doss Goverdhan Doss Vaishnav College (accredited at 'A' grade by NAAC), one of the premier institutions in Chennai