International Journal of Engineering & Technology, 7 (4.6) (2018) 86-90

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Visual Feature Based Image Forgery Detection

D. Vaishnavi[1], D. Mahalakshmi[2,] Venkata Siva Rao Alapati [3]

[1]Dept. of CSE,Vardhaman College of Engineering, Hyderabad, Telangana, India,
[2]Dept. of IT, A.V.C. College of Engineering, Tamilnadu, India
[3]Department of Computer Science and Engineering MLR Institute of Technology, Hyderabad
**Corresponding author E-mail:vaishume11@gmail.com*

Abstract

In present days, the images are building up in digital form and which may hold essential information. Such images can be voluntarily forged or manipulated using the image processing tools to abuse it. It is very complicated to notice the forgery by naked eyes. In particular, the copy move forgery is enormously demanding one to expose. Hence, this paper put forwards a method to determine the copy move forgery by extracting the visual feature called speed up robust features (SURF). In the direction to quantitatively analyze the performance, the metrics namely false positive rate and true positive rate are estimated and also comparative study is carried out by previous existing methods.

Keywords: *Image splicing forgery; local binary pattern; SVM; BPNN; combined k-NN.*

1. Introduction

The digital/computerized images has turned into an imperative information source, due to the reputation of internet, increasing ease of use digital cameras and photo editing softwares. However, the popularity of the digital images causes tricky digital forgeries which corrupts the genuineness of images. Currently, many case of image forgeries can be seen in our society with regards to news, legal evidence, business, military affairs etc., A tool is required by the people to recognize whether image is genuine or tampered, when the image contents are being doubtful. Hence, the various methods of tampering detection have been offered. In era, fragile watermarking [1–5] and digital signatures [6–8] were used to distinguish the image forgeries.

In recent years, researchers are detecting the forgeries without any prior knowledge or additional information [9] and there are many kinds of forgeries such as object or region hiding and increase the number of same objects, object addition and change the appearance of object etc. In which, object or region hiding and increase the number of same object is called copy move forgery and it can be done by copying a region or object in image and pasting it into another part of image itself. This sort of forgery is hard to recognize by visual observation. Therefore this paper proposes a technique to detect such kind of forgeries using the SURF features.

The remaining part of this paper is structured as follows: Section 2 provides the existing work related to forgery detection, Section 3 furnishes the methodology of the proposed work, Section 4 discusses the experimental results and finally Section 5 concludes the paper.

2. Related works

The copy move forgery can be detected either by block based method or visual feature based method. Even though, there are huge volume of block based forgery detection approaches available, they are consuming too much of time to detect the forgery and are not much exciting [10–12]. Quite the reverse, the feature based method can be able to detect the forgeries effectively in few seconds. In [13] Scale Invariant Feature Transform (SIFT) features are extracted and key point matching is done by selecting the points which are far from the 11×11 pixel window to detect forgery. In [14], the authors has detected the forgery more effectively using the SIFT features by offering a g2NN test and the same features are used in [15] by improving the detection algorithm. The scheme in [16] extracted MPEG-7 visual invariant signatures. In [17], a method utilized SURF algorithm to find the forgery and matching is performed by selecting the features using best bin search algorithm. In [18], the keypoints of accelerated segment test (FAST) are identified and descriptors of Binary Robust Independent Elementary Features are obtained. The scheme in [19], authors extracted the rotation-invariant DAISY descriptor to detect a cloned region. The authors of [20], improved the DAISY descriptors by extracting them at the keypoints obtained by difference of gaussian (DoG). The methods in [21], [22], extracted the SIFT features from the approaximate coefficients of the discrete wavelet transform (DWT) and dyadic wavelet transform (DyWT) respectively. The method in [23], extracted the contrast context histogram features to detect the forgery. In [24], authors detected the forgery using the maximum stable extremal regions (MSER).

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

3. Proposed method

The proposed forgery detection method consists of three steps: feature extraction, feature matching, and tamper detection. SURF algorithm is said to be faster and at same time robust to scale, noise and geometric deformation etc. So, SURF algorithm is employed to extract the features for detecting the forgery. .

3.1. Feature extraction

The SURF finds the interest points by employing Hessian based blob detector. The determinant of a Hessian matrix is a representation of the local change around the area and its response.

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

where,

$$L_{xx}(x,\sigma) = I(x) * \frac{\partial^2}{\partial x^2} \mathrm{g}(\sigma)$$

where, $L_{xx}(x,\sigma)$, $L_{yy}(x,\sigma)$ and $L_{xy}(x,\sigma)$ are gaussian second order derivative convolution of image points. The convolutions are very expensive to compute and it is approximated and its computation is turned up fast by the integral images and approximated kernels. *I(x)* is an integral image where each point $x = (x, y)^T$ is stored by summing all pixels in a rectangular area between origin and *x*.

$$I(x) = \sum_{i=0}^{i\le x} \sum_{j=0}^{j\le y} I(x,y)$$

Generally, the keypoint is extracted after the scale space analysis. In SURF algorithm, scale space is achieved by approximating the box filter with Laplacian of Gaussian along and convolving an image by various the size of box filter. Later the scale space is generated and determinant of the Hessian matrix is estimated to identify extremas. It finds the extemas as key points if determinant of the Hessian matrix is positive; which means both the Eigen values are of the same sign. The approximate determinant of the Hessian matrix is calculated by

$$\det(H_{app}) = D_{xx}D_{yy} - (wD_{xy})^2$$

The *w* term is energy conservation for the Gaussians and it is theoretically sensitive to scale but it can be kept constant at 0.9.

A circular area is constructed around the keypoints to find the dominant orientation. Then, Haar wavelets are used for the orientation assignment. It also increases the robustness and decreases the computational cost. Haar wavelets are filters that detect the gradients in *x* and *y* directions. So as to make rotation invariant, an orientation for the interest point is identified and a circle segment is rotated about the interest point. The maximum value is elected as a dominant orientation for that point.

A square region around a keypoint is formed to compute the descriptors and it is further segregated into *4×4* sub-regions. The Haar wavelet responses are computed and *4* responses are collected from the each sub-regions. Therefore, the dimension of the descriptor is *4×4×4=64*. Here, the terms $d_x, d_y, |d_x|$ and $|d_y|$ are the horizontal and vertical responses and their absolute responses respectively.

$$v_{subregion} = [\sum d_x, \sum d_y, \sum |d_x|, \sum |d_y|]$$

3.2. Feature Matching

Next, feature matching step is performed. This can be done by determining ratio between the nearest neighbours and it is considered as initial matches whose ratio is less than that of the ratio threshold T1. Further, the final matches are stored if distance between the neighbours is greater than the distance threshold T2. Then, the hierarchical clustering is applied to isolate the pasted and copied region points using 'ward' linkage method.

Sometimes false matches may be in the list of detected matching key points of forged regions. If it is available, it may form the vulnerable issue regarding the genuineness of an image and also it directs to inaccurate evaluation of transformation. Therefore, such false matches are need to be avoided and are discarded using the algorithm of random sampling consensus (RANSAC) [25]. This algorithm first selects the two or more matched points at random and computes the homography matrix. The rest of the points are transformed with respect to homography matrix and are analyzed by calculating the distance relating to corresponding matching points. Then it is certified either as outlier or inlier depends on the distance lies over or below a threshold. It is continued for N number of times until the maximum possible number of inliers found. In our experiment the value of N is fixed to 500 and distance threshold for 0.05.

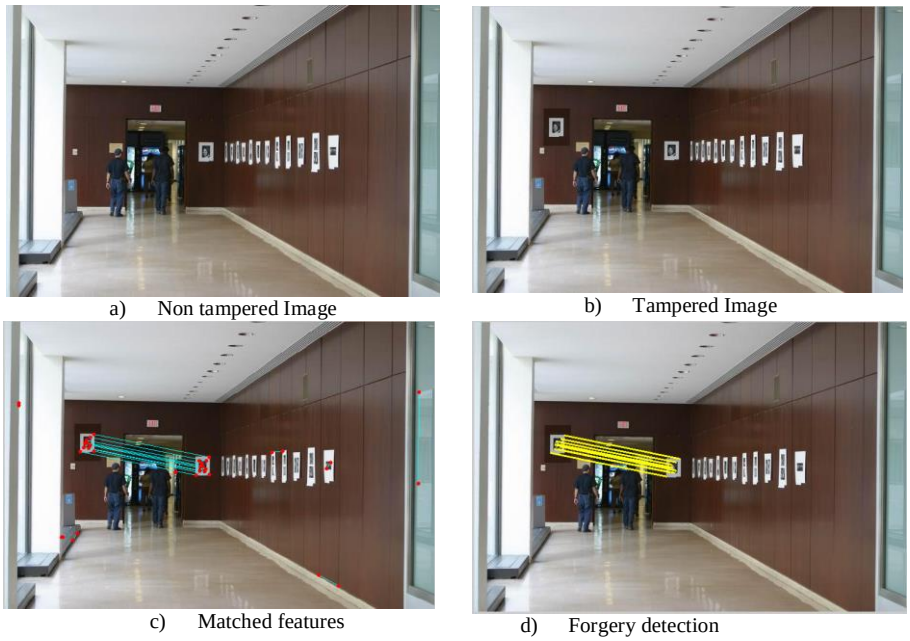
4. Experimental results and discussion

In this experiment, to quantify the performance of the proposed system, the tampered images and original images are adopted from MICC-F220 and MICC-F2000 databases. Where MICC-F220 dataset contains 110 original and 110 tampered images and MICC-F2000 dataset contains 700 tampered and 1300 original images of 2048 pixels × 1536 pixels. This second data set, the size of the forged parts covers on average 1.12% of an image. This proposed system is evaluated on the basis of False Positive Rate (FPR) and True Positive Rate (TPR) are given as follows:

$$TPR \text{ in } \% = \frac{\#\text{ tampered images correctly detected}}{\#\text{ tampered images}}$$

$$FPR \text{ in } \% = \frac{\#\text{ orignal images detected as tampered}}{\#\text{ original images}}$$

The sample result of tamper detection is shown in Fig. 1, in which, Fig.1 a) is an original, non-forged image and Fig.1 b) is tampered image which is forged by copying and pasting the women in the region. Fig. 1 c) shows the matching features detected by the proposed method and Fig. 1 d) shows the final result of detected forged image. Fig. 2 and Fig. 3 shows the resultant images that are detected as original being original and are detected as forged being original. Fig. 4 shows the detection results in the presence of scaling, rotation and combination of both attacks.



a) Non tampered Image b) Tampered Image

c) Matched features d) Forgery detection

Fig.1 Results of proposed method

Table 1: Performance comparison with previous methods on MICC-F220 Dataset

Methods	**FPR %**	**TPR %**
DOG+DAISY [20]	9.09	85.91
Proposed method	**9.09**	**81.81**
DyWT+SIFT[21]	10.00	80.00
DyWT[12]	4.00	74.00
DWT+SIFT [22]	2.00	66.00

To quantify the performance of the proposed system, the experiment is carried out on MICC-F220 database and it produced 81.81% of TPR and 9.09% of FPR. The results of the proposed system is compared with the previous copy move forgery detection methods [20] [21] [12] and [22] and is tabulated in the Table 1. The proposed method is better in terms of TPR except the method [20] and it is achieved a lower value in terms of FPR.

The experiment is also carried out on the MICC-F2000 dataset and performance is evaluated using TPR and FPR measures. The proposed system is achieved 6.92% of FPR and 92.85% of TPR. These results are analyzed with the existing systems and its results are tabulated in the Table 2. It furnishes that performance of the proposed method is well improved in terms of FPR when compared with all the methods and it is improved some extend in terms of TPR compared to the Areej et. al [24].

Table 2: Performance comparison with previous methods MICC-F2000

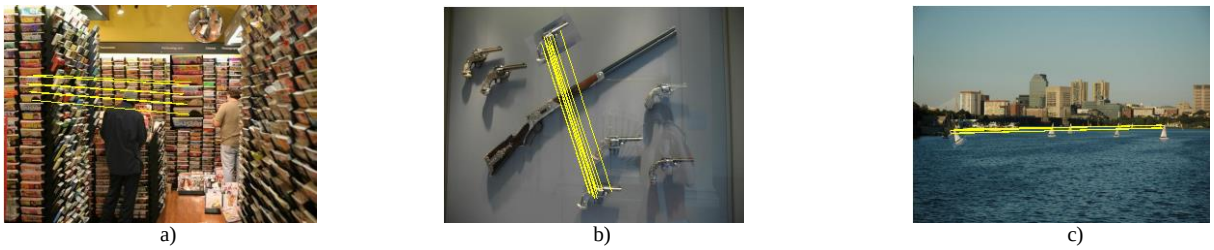
Methods	**FPR %**	**TPR %**
Proposed method	**6.92**	**92.85**
Areej et. al [24]	8.00	92.00
Amerini et. Al 2013 [15]	9.15	94.86
Amerini et. al 2011 [14]	11.61	93.42



Fig. 2: Images detected as original that are being original



Fig. 3: Images detected as forged that are being original



a) b) c)

Fig.4: Detection result subject to geometric transformations a) scaling, b) Rotation and c) Scaling and Rotation



a) Quality factor 50 b)) Quality factor 75

Fig. 5: Tampered image detection with JPEG compression



Fig. 6: Tampered image detection with noise 0.02

In addition, the robustness of the proposed system is tested for JPEG compression and noise. In this experiment, the quality factor 50 & 75 and variance of 0.02 zero mean noise is applied for JPEG compression and noise attacks. Fig. 5-6 shows the detection results in the presence of compression and noise addition attacks. It can be seen that the proposed system is highly robust to compression and it is slightly affected by the noise addition attack

5. Conclusion

The proposed passive approach for copy move forgery detection is implemented successfully by extracting the SURF features. To facilitate the quantitative analysis of performance of proposed method, an experiment is conducted on images of MICC-F220 dataset, its results are evaluated by the metrics TPR and FPR and it is achieved a result of 81.81% of TPR, 9.09% of FPR, 92.85% of TPR and 6.92% of FPR on MICC-F220 and MICC-F2000 dataset respectively. These results are comparatively analyzed with the existing methods and is concluded that the proposed approach is achieved a good TPR and FPR results in terms of MICC-F220 and MICC-F2000 datasets respectively.

References

[1] Shivani, S., Singh, D., and Agarwal, S. (2013) DCT Based Approach for Tampered Image Detection and Recovery Using Block Wise Fragile Watermarking Scheme. In Pattern Recognition and Image Analysis, pp 640–647, Springer.

[2] Vaishnavi, D., and Subashini, T. (2015) Image Tamper Detection Based on Edge Image and Chaotic Arnold Map, Indian Journal of Science and Technology 8, 548–555.

[3] He, H., Zhang, J., and Chen, F. (2008) A self-recovery fragile watermarking scheme for image authentication with superior localization, Science in China Series F: Information Sciences, SP Science in China Press 51, 1487–1507.

[4] Rawat, S., and Raman, B. (2011) A chaotic system based fragile watermarking scheme for image tamper detection, AEU-International Journal of Electronics and Communications, Elsevier 65, 840–847.

[5] Vaishnavi, D., and Subashini, T. (2015) Fragile Watermarking Scheme Based on Wavelet Edge Features, JOURNAL OF ELECTRICAL ENGINEERING & TECHNOLOGY, KOREAN INST ELECTR ENG 901 KSTC, 635-4 YEOKSAM-DONG, GANGNAM-GU, SEOUL, 135-703, SOUTH KOREA 10, 2149–2154.

[6] Lu, C.-S., and Liao, H.-Y. M. (2003) Structural digital signature for image authentication: an incidental distortion resistant scheme, Multimedia, IEEE Transactions on 5, 161–173.

[7] Zhang, H.-B., Yang, C., and Quan, X.-M. (2004) Image authentication based on digital signature and semi-fragile watermarking, Journal of Computer Science and Technology, Springer 19, 752–759.

[8] Wang, X., Xue, J., Zheng, Z., Liu, Z., and Li, N. (2012) Image forensic signature for content authenticity analysis, Journal of Visual Communication and Image Representation, Elsevier 23, 782–797.

[9] Farid, H. (2009) Image forgery detection–A survey, Citeseer.

[10] Fridrich, A. J., Soukal, B. D., and Luk, A. J. (2003) Detection of copy-move forgery in digital images. In in Proceedings of Digital Forensic Research Workshop, Citeseer.

[11] Wu, Y., Deng, Y., Duan, H., and Zhou, L. (2014) Dual tree complex wavelet transform approach to copy-rotate-move forgery detection, Science China Information Sciences, Science China Press 57, 1–12.

[12] Muhammad, G., Hussain, M., and Bebis, G. (2012) Passive copy move image forgery detection using undecimated dyadic wavelet transform, Digital Investigation, Elsevier 9, 49–57.

[13] Pan, X., and Lyu, S. (2010) Region duplication detection using image feature matching, Information Forensics and Security, IEEE Transactions on, IEEE 5, 857–867.

[14] Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., and Serra, G. (2011) A sift-based forensic method for copy–move attack detection and transformation recovery, Information Forensics and Security, IEEE Transactions on, IEEE 6, 1099–1110.

[15] Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Del Tongo, L., and Serra, G. (2013) Copy-move forgery detection and localization by means of robust clustering with J-linkage, Signal Processing: Image Communication, Elsevier 28, 659–669.

[16] Kakar, P., and Sudha, N. (2012) Exposing postprocessed copy paste forgeries through transform invariant features, Information Forensics and Security, IEEE Transactions on, IEEE 7, 1018–1028.

[17] Mishra, P., Mishra, N., Sharma, S., and Patel, R. (2013) Region Duplication Forgery Detection Technique Based on SURF and HAC, The Scientific World Journal, Hindawi Publishing Corporation 2013.
[18] Zhu, Y., Shen, X., and Chen, H. (2015) Copy-move forgery detection based on scaled ORB, Multimedia Tools and Applications, Springer 1–13.
[19] Guo, J.-M., Liu, Y.-F., and Wu, Z.-J. (2013) Duplication forgery detection using improved DAISY descriptor, Expert Systems with Applications, Elsevier 40, 707–714.
[20] Jiming ZHENG, P. L. (2014) Detection of Copy-move Forgery in Digital Image using DAISY Descriptor, Journal of Computational Information Systems, Binary Information Press 10, 9369–9377.
[21] Anand, V., Hashmi, M. F., and Keskar, A. G. (2014) A copy move forgery detection to overcome sustained attacks using dyadic wavelet transform and sift methods. In Intelligent Information and Database Systems, pp 530–542, Springer.
[22] Hashmi, M. F., Hambarde, A. R., and Keskar, A. G. (2013) Copy move forgery detection using DWT and SIFT features. In Intelligent Systems Design and Applications (ISDA), 2013 13th International Conference on, pp 188–193, IEEE.
[23] Vaishnavi, D., and Subashini, T. (2015) A passive technique for image forgery detection using contrast context histogram features, International Journal of Electronic Security and Digital Forensics, Inderscience Publishers (IEL) 7, 278–289.
[24] Alfraih, A. S., Briffa, J. A., and Wesemeyer, S. (2014) Cloning localization based on feature extraction and k-means clustering. In Digital-Forensics and Watermarking, pp 410–419, Springer.
[25] Fischler, M. A., and Bolles, R. C. (1981) Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography, Communications of the ACM, ACM 24, 381–395.