Automated Forensic Method for Copy-Move Forgery Detection based on Harris Interest Points and SIFT Descriptors

B.L.Shivakumar
Department of Computer Applications
S.N.R. Sons College
Coimbatore – 641006, Tamilnadu

Dr. S.Santhosh Baboo
PG & Research Dept. of Computer Applications
D.G. Vaishnav College
Chennai – 600106, Tamilnadu

ABSTRACT
We are undoubtedly living in an age where we are exposed to a remarkable array of visual imagery. Nowadays, accepting digital images of official documents is common practice. Image authenticity is important in many social areas. For instance, the trustworthiness of photographs has an essential role in courtrooms, where they are used as evidence. In the medical field, physicians make critical decisions based on digital images. The technology today makes it convenient to quickly exchange contracts, photographs or other documents. While we may have historically had confidence in the integrity of this imagery, today's digital technology has begun to erode this trust. With the advent of low-cost and high-resolution digital cameras, and sophisticated photo editing software, digital images can be easily manipulated and altered. It is possible to change the information represented by an image and create forgeries, which are indistinguishable by naked eye from authentic photographs and documents. In the proposed method Harris Interest Point detector along with SIFT descriptors are used to detect copy-move forgery. KD-Tree is used for matching.

Keywords
Copy-Move Forgery, Harris interest point, SIFT, KD-tree.

1. INTRODUCTION
Computer forensics is one of the largest growth professions of the 21st century. The rapid growth in computer technology with the constant computerization of business processes has created new opportunities for computer criminals. Study after study has revealed that computer-based criminal activities are costing business and government organizations billions of dollars every year. Nowadays the soaring increase in the number of internet user has resulted in accepting digital images as official documents and easy way of communication. Digital images are used in court rooms as evidence of crime and are also used by physicians. An unfortunate concern today is that digital images could be damaged, destroyed, or misappropriated by a discontented individual. Information integrity is an important factor in digital images. The advent of digital pictures and the technology today makes this authenticity uncertain. Anyone with access to a computer and with little knowledge in software, such as Adobe Photoshop can create a forged image. The tampering with photographic images is not new. Tampering with photographic images dates back to the time when permanent photographic images were first created. Vladimir Ilyich Lenin was one of the earliest instigators of photographic image tampering. Recently, (September 2010) Egypt's state-run newspaper, *Al-Ahram*, published the Tampered photo (Figure 1) of Egyptian President Mubarak walking with Israeli, US, Palestinian and Jordanian leaders during the latest Middle East peace talk. However, the photo published was a good example of tampering.

Fig. 1. The photo (right) is a tampered with original (left)

With the emergence of digital forensics over the past few years has helped to restore some trust in the field of digital imagery. Digital forensics [1], deals with developing systems in the absence of watermarks [2] or signatures inserted in the image. Basically, the digital image forgery detection methods are classified into Active Digital Image Forensics and Passive Digital Image Forensics or Blind Digital Image Forensics [3]. Unlike the active method such as digital watermarking and digital signature, the passive approach does not rely on pre-embedded information. Forgery detection aims to tell whether the digital image content is authentic without image forgery operations.

Copy-move forgery, as depicted in Figure 2, is one type of forgery in which one part of the image itself is copied and pasted into another part of the same image. Since the copied region are from the same images, some components (eg. colour and noise) will be compatible with the rest of the image and therefore will

not be detectable using methods that look for incompatibilities in statistical measure in different parts of the image [4].

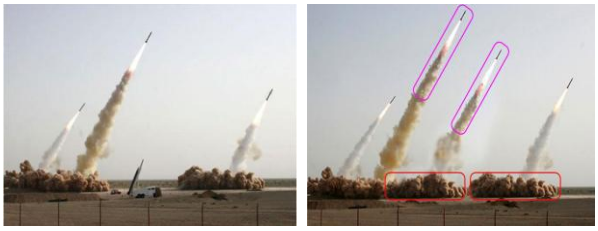

Figure 2. An example of copy-move forgery that appeared in press in July, 2008.The original image (on the left) shows three original image and the tampered image (on the right) shows four Iranian missiles; two different sections (encircled in red and purple, respectively) replicate other image sections by applying a copy-move attack.

A copy-move forgery introduces a correlation between the original image area and the pasted one, hence it is difficult to identify by naked eyes. Several techniques are discussed in literature to identify copy-move forgery [5], [6]. The simplest approach to detect a copy-move forgery is to use an exhaustive search as pointed in [7]. In copy-move forgery the cloned region can be of any shape and location, it is computationally infeasible to search all possible image locations and sizes as pointed in this method. The authors in [8] introduced a sorted neighborhood approach based on DWT (Discrete Wavelet Transformation) and SVD (singular Value Decomposition). These algorithms are based on block-matching are computationally complex and some algorithms are weak to locate the copy-move region after-copying manipulations, such as lossy compression, blurring or combination of these operations. To improve the detection time, the authors in [9] applied Principle Component Analysis (PCA) on the small blocks to get a reduced dimension representation. A similar approach is proposed in [10] where Fourier Mellin Transform is applied to each block. The authors in [11] 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 Regressive coefficients and Artificial Neural Network(ANN).

It is often necessary to resize, stretch, or rotate portions of an image to create a convincing forgery. Good forgery detection method should be robust to some types of transformations, such as scaling, rotations and JPEG compression and Gaussian Noise addition. Recently, an attempt was made in [12] to identify copy-move forgery using Zernike moments. Their method detects duplicated region rotated some angle before it is pasted. The system was weak against scaling and other type of tampering based on affine transform. In the recent past, the local features such as SIFT [13], SURF [14], and region based features such as the MSER (Maximally Stable External Regions [15] are used for recognition and localization of objects due to their robustness to several geometrical transformations. A detailed comparison of several local descriptors is provided in [16] [17]. SIFT features considered to be good solution for object recognition because of their relatively low computational cost and robust performance. SIFT features are used for copy-move forgery detection in [18], [19], [20].

2. PROPOSED METHOD

Good copy-move forgery detection should be robust to some type of transformations. Most of the existing methods are time consuming and do not deal with all transformation. One of the main strengths of SIFT features are their scale invariance. However, the scale-space analysis required for the calculation of the SIFT feature point positions is too slow for visual related applications. In this paper we focus on detection of copy-move forgery which is robust to some types of manipulation based on Harris corner detector [22] and SIFT descriptors, using the technique proposed in [21]. A simple schematization of the whole system is shown Figure 3.

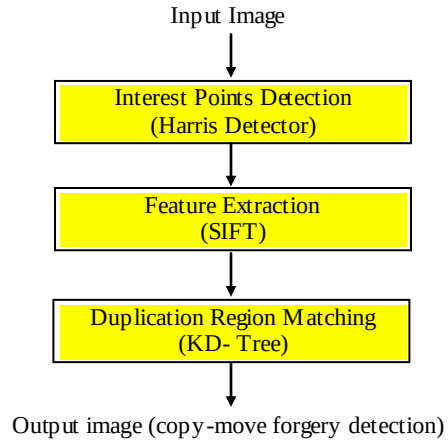

Figure 3. Overview of the proposed system.

2.1 Interest Point Detection

Different Interest points detector have been proposed and used based on the field of applications. The fast, robust and rotation invariant, Harris detector is widely used in many computer vision applications which uses the autocorrelation function to determine locations where the change of signal in one or two directions. A matrix related to the auto-correlation function is computed:

$$C(x, \sigma_I, \sigma_D) = \sigma_D^2 G(x, \sigma_I) * \begin{pmatrix} L_x^2(x,\sigma_I) & L_x L_y(x,\sigma_I) \\ L_x L_y(x,\sigma_I) & L_y^2(x,\sigma_I) \end{pmatrix} \quad (1)$$

where σ_D is the derivation scale, σ_I is the integration scale, G is the Gaussian and L is the image smoothed by a Gaussian kernel. This matrix has two Eigen values that are the principal

curvatures of the auto-correlation function. When the two eigenvectors are very small then there is no structure exists. If one is large and another one is small, there is an edge like structure. If both of them are very large and distinct, there is a corner like structure. Edges and interest points can be computed based on:

$$det(C) - \alpha . trace^2(C) < T_E, \quad (2)$$

and

$$det(C) - \alpha . trace^2(C) > T_C. \quad (3)$$

Edges are computed based on equation (2), where α is the coefficient of the Harris function and T_E is the threshold of the Harris function ($T_E < 0$). The edge detection is carried out at the first scale. Interest points can be detected by using eq. (3), T_C is the threshold for interest points ($T_C > 0$).

2.2 Feature Extraction

The Feature extraction is the main for any system which requires matching. The extracted features should be well separated in the feature space to produce effective discrimination between images. In this work the features is extracted using SIFT. The feature descriptor is computed as a set of orientation histograms on 4 x4 pixel neighbourhoods.

2.3 Key Point Matching

In our system to identify the duplication region the KD-tree [23] 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.[24] The KD-tree is commonly used structure for searching for nearest neighbors. The KD tree pre-processes data into a data structure allowing us to make efficient range queries.

3. EXPERIMANTAL RESULTS

The proposed method have been implemented using Matlab 7.6 in a computer of CPU 2.20 GHz with memory of 3 GB. The fast Harris detector along with SIFT descriptors are used to detect interest point and descriptors. The main task in any object recognition is matching the similarity between two feature points. For this KD-tree algorithm is used in our system. The images have been selected from the dataset proposed in [24]. Since the image size is very important for any detection algorithms, six different images which are considered to be more challenging for copy-move forgery detection with different resolution and different size of copied area are used in our experiment. The original images are shown in Figure 4. Three images are of high resolution of more than 2000 x 1600 pixels and three images are of low resolution. The copied region has basically the same appearance of the original one, therefore the keypoints extracted in the duplicated region will be similar to the original ones. Therefore, matching among the features can be adopted for the task of determining possible tampering.

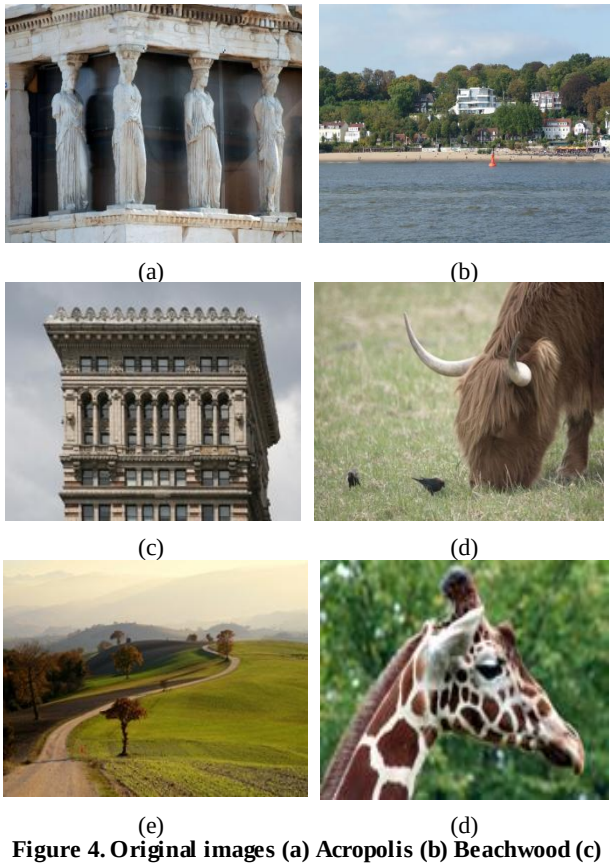

Figure 4. Original images (a) Acropolis (b) Beachwood (c) Building (d) Cattle (e) Tree and (f) Giraffe

Here, we report some experimental results on images where a copy-move attack has been performed. In this case the forged region is selected according to the specific goal to be achieved and, above all, paying attention to perfectly conceal a modification, where the alteration are not recognizable at least at the first glance and forensic tool could help to investigations. For instance the image *Acropolis* is forged with the right most statues which is marked with ellipse, the image *Beachwood* is forged with a green patch to conceal a building and the image. In the image *Building* two small statues on the left and right most broad pillars are copied and pasted in the second and third broad pillars. The crow and small green patch is copied and pasted in the image *Cattle*. T*ree* is modified with another tree and the neck marking in *Giraffe* is forged. The forged area is highlighted with circle or ellipse in the top row of Figure 5 and Figure 8. The three tampered images *Acropolis*, *Beachwood* and *Tree* are affected with large area of forged region, while the images *Building*, *Cattle* (neck region) and *Giraffe* (neck region) is affected with small region of forged area. Further, in the image *Building* and C*attle* more than one region is forged. The image with its resolution is listed in Table I.

Table I. Test images with their resolutions

Image	Resolution
Acropolis	3872 *x* 2592
Beachwood	3264 *x* 2448
Building	2660 *x* 2104
Cattle	1280 *x* 854
Tree	1024 *x* 683
Giraffe	800 *x* 533

A. Test for forgery detection

For the proposed method the Harris threshold is set as 300 for high resolution images and as 50 for low resolution images. First the proposed method is analyzed to determine the best settings for the cut-off threshold T_h (matching) for the images. The Interestingly, by decreasing the Harris threshold the number of keypoints increased, which resulted in more match points and subsequently detection time also increased. The results indicate that the proposed method detects copy-move forgery efficiently. The Figure 5, shows high resolution tampered images (top row), the keypoints extracted for the tampered image (middle row) and the detection result(bottom row)

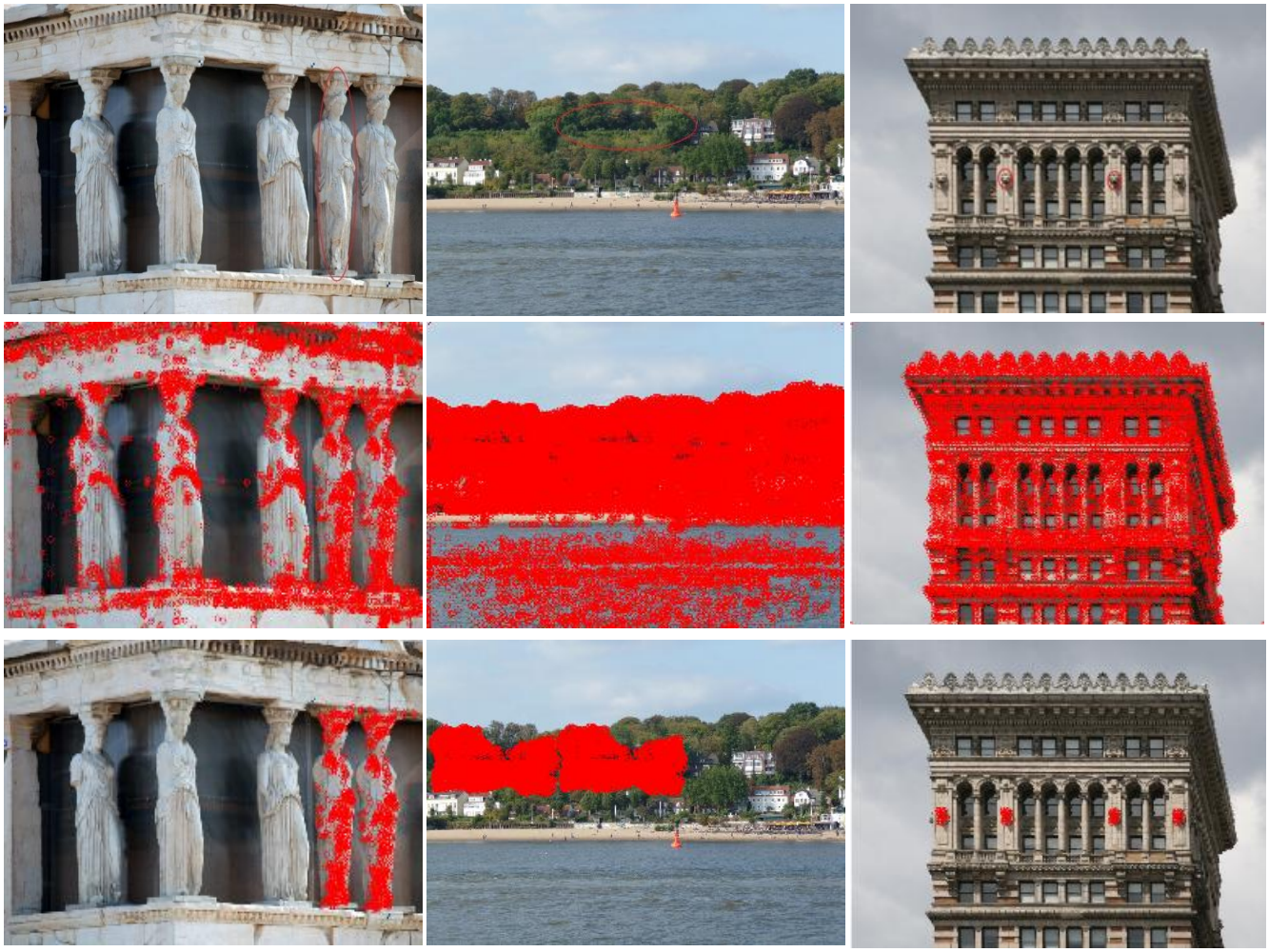

Figure 5. The forged images are in the top row. The forged region is highlighted with circle or ellipse. The keypoints extracted for the tampered images are shown in middle row. The last row shows the detected region. From left to right: *Acropolis* **(large copied region),** *Beachwood* **(large copied region) and** *Building* **(small region with two forged area).**

In Table II, the optimum matching threshold for each image, the number of keypoints extracted and the detection time (in seconds) are reported for three images with high resolutions.

Table II. Shows the optimum threshold (matching) , the number of keypoints extracted, the number of keypoints matched and the detection time for each image.

Image	Threshold T_h	No. of Keypoints	Matches	Detection Time(Sec)
Acropolis	0.15	5339	1144	957.873
Beachwood	0.06	18430	4132	1293.143
Building	0.10	9494	103	2685.054

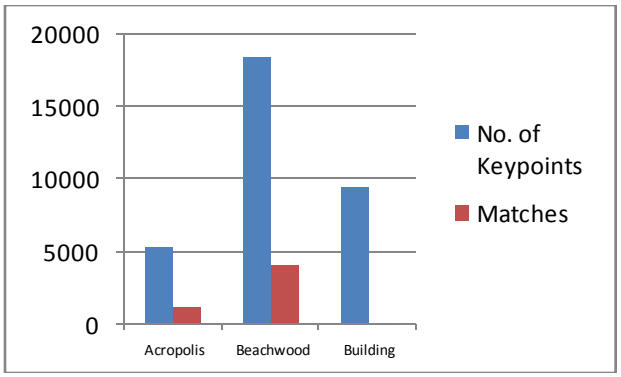

Figure 6. Comparison between the number of keypoints extracted for high resolution images and the number of keypoints matched.

A high number of matches are fundamental in order to identify the forged region. Note for image *Building* the number of matches is very less. This is mainly because a small region is coloned in this image.

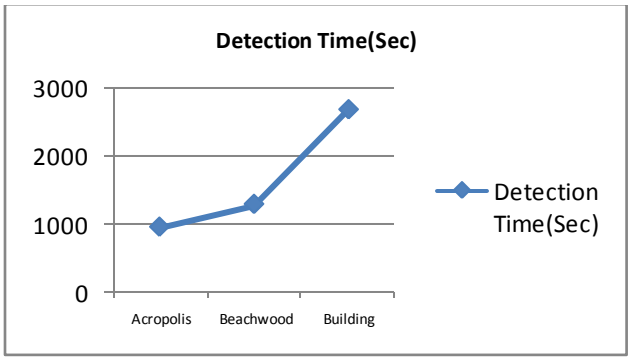

Figure 7. Time taken (seconds) to detect the duplicated region.

To analyze the performance of the proposed technique, the experiment was repeated with low resolution images. It is interesting situation concerns the individuation of forged region for the image named *Giraffe* and *Tree*, the method able to detect a sufficient number of matched keypoints. On the contrary, for the image named *Cattle*, where two regions are forged, the method was able to detect only one forged region for the given Harris threshold(300). This is basically due to lesser number of keypoints extracted. Therefore, we reduced the Harris threshold to 50, to have sufficient number of keypoints for the low resolution images. The result indicates the proposed method detects the forged region efficiently for images with low resolution, when there is more keypoints. In Table III, the number of keypoints extracted and the detection time (in seconds) and the optimum matching threshold for each image are reported.

Table III. Shows the optimum threshold (matching) , the number of keypoints extracted, the number of keypoint matched and the detection time for each image.

Image	Threshold T_h	No. of Keypoints	Matches	Detection Time(Sec)
Cattle	0.08	4482	53	645.063
Tree	0.13	2274	37	242.517
Giraffe	0.12	2193	27	182.707

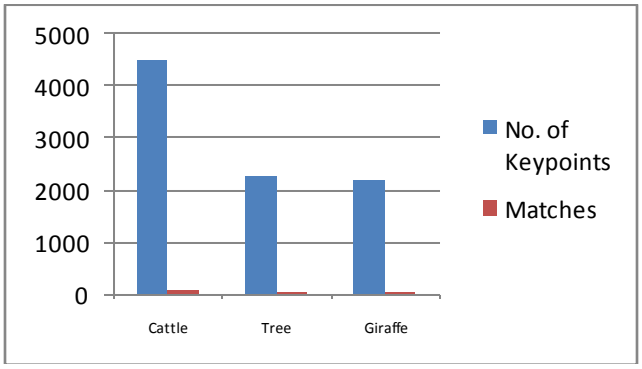

Figure 8. Comparison between the number of keypoints extracted for low resolution images and the number of keypoints matched.

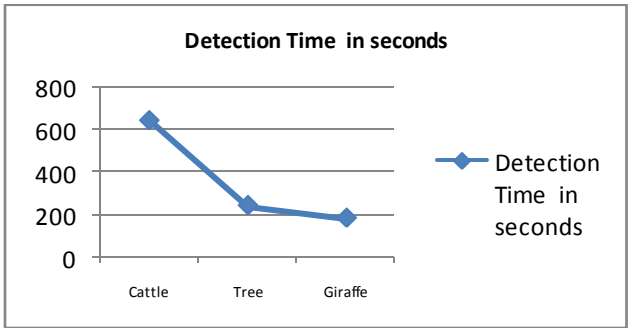

Figure 9. Time taken (seconds) to detect the duplicated region

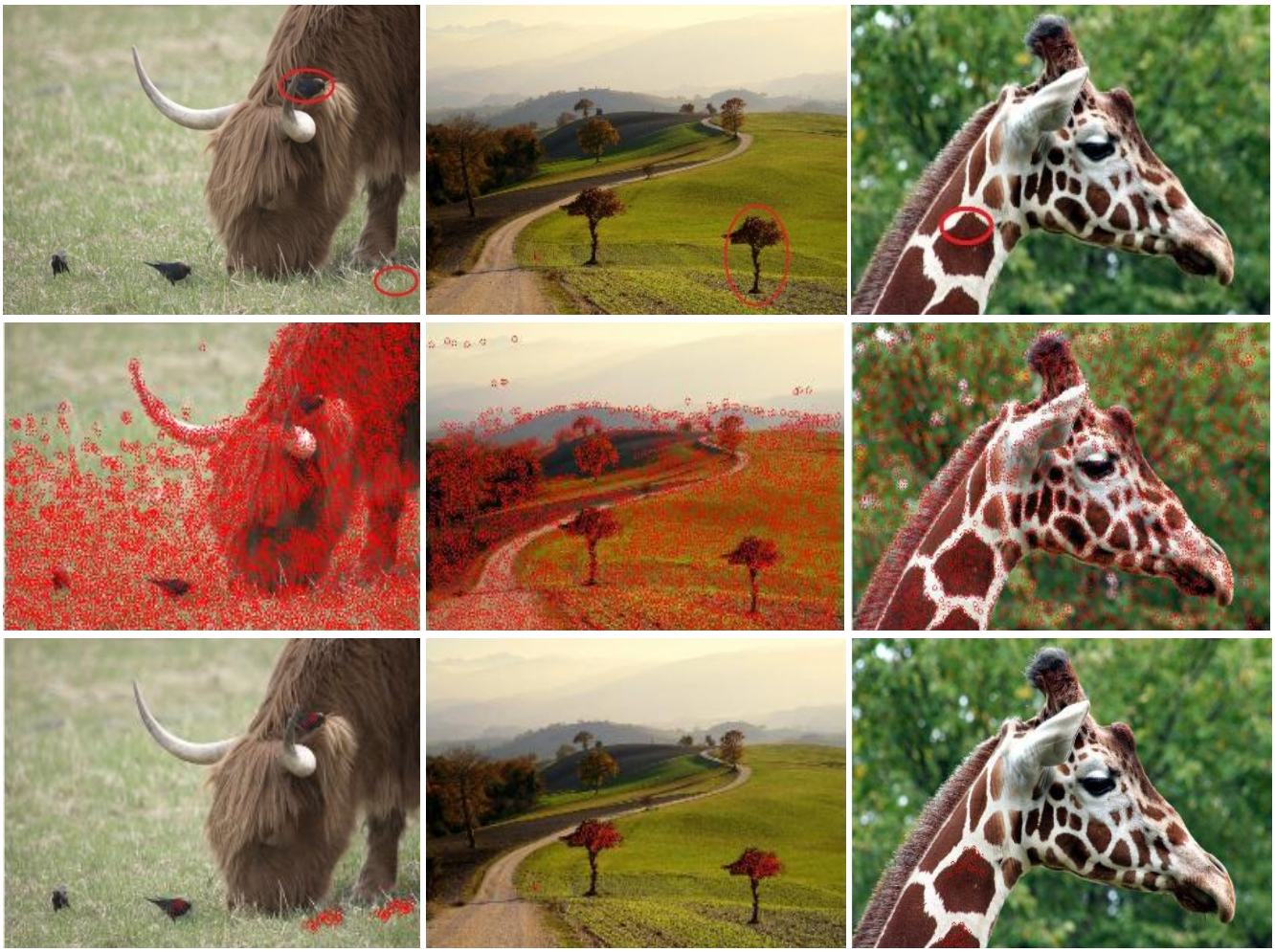

Figure 10. The forged images are in the top row. The forged region is highlighted with circle or ellipse. The keypoints extracted for the tampered images are shown in middle row. The last row shows the detected region. From left to right: *Cattle* **(two small copied region),** *Tree* **(large copied region) and** *Giraffe* **(small forged region).**

B. Test on multiple copied regions

The proposed method was also analyzed to determine the performance of tampered images which have multiple copies of the same region. To address this problem two images A*cropolis* with high resolution and the image *Tree* which is low resolution image was considered. The right most statues in the image *Acropolis* and a tree in the image *Tree* was copied and pasted in several different positions over the original image. Figure 11 shows the detection result obtained with multiple copied regions for images *Acropolis* and *Tree* respectively.

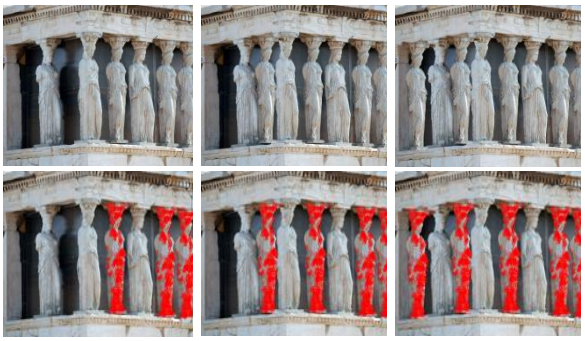

Figure 11. Examples of tampered images (*Acropo*lis) with multiple doning are shown in the first row and the detection results are reported in second row.

Table IV. Shows the number of keypoints extracted, the number of keypoints matched and the detection time for *Acropolis* after multiple forgery.

No of Forgery	No. of Keypoints	Matches	Detection Time(Sec)
One	5339	1114	957.873
Two	6034	1760	1109.366
Three	6687	2388	1102.753
Four	7378	3017	1382.903

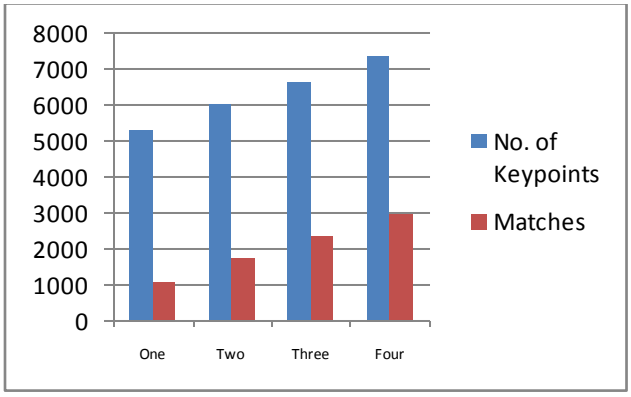

Figure 12. Comparison between the number of keypoints extracted for high resolution images and the number of keypoints matched

It is interesting to note that the number of keypoints and the number of matched points proportionally increased for the image *Acropolis*, where the lighting of the image is same throughout the image. On contrary for *Tree* with multiple forgery the number of matched points have not increased proportionally because the image is not flat and the lighting spread throughout the image is not same.

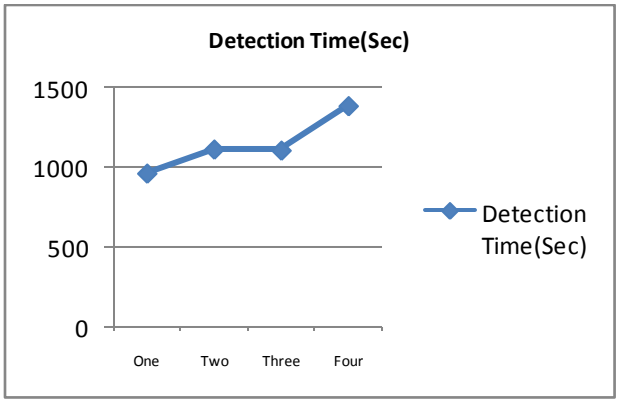

Figure 13. Time taken (seconds) to detect the duplicated region with multiple forgeries.

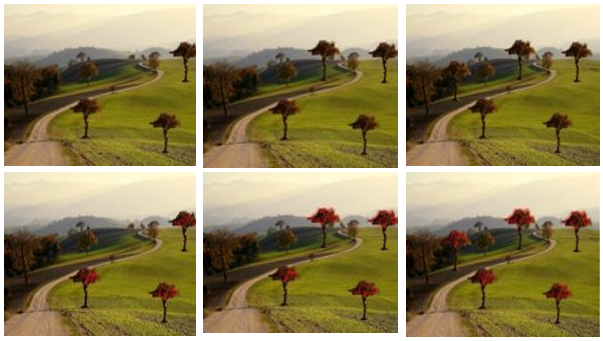

Figure 14. Examples of tampered images (*Tree*) with multiple doning are shown in the first row and the detection results are reported in second row.

Table V. Shows the the number of keypoints extracted, the number of keypoints matched and the detection time for *Tree* after multiple forgery.

No of Forgery	No. of Keypoints	Matches	Detection Time(Sec)
One	2274	37	242.517
Two	2788	39	228.79
Three	2800	80	232.205
Four	2803	98	225.851

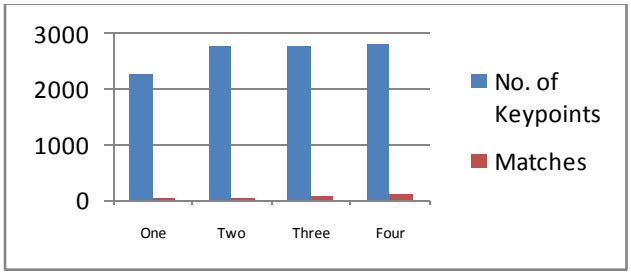

Figure 15. Comparison between the number of keypoints extracted for high resolution images and the number of keypoints matched

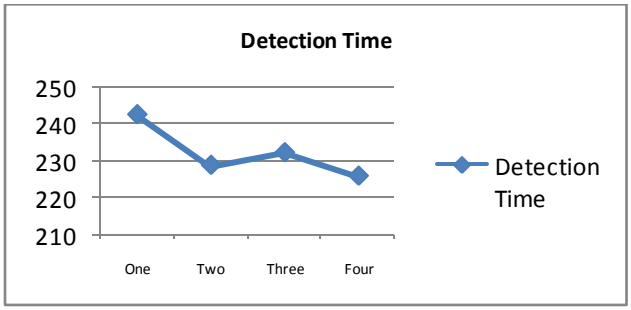

Figure 16. Time taken (seconds) to detect the duplicated region with multiple forgeries.

C. *Test on Transformation*

In this section, we analyze the performance of our system to test images which has undergone some transformation. The forged images are obtained in the image *Acropolis* for which scaling (symmetric/asymmetric) is applied. Table III summarize the geometric transformations for the attack applied to the coloned part in the image *Acropolis*. For an example in the attack F, the *x* and *y* axes are scaled by 20%.

Table VI. Different combinations of geometric transformation (scaling) applied to Acropolis

attack	s_x	s_y	No. of keypoints points	Matched Points	Detection Time (Sec)
a	1.0	1.1	5340	714	1001.084
b	1.1	1.0	5416	742	1335.734
c	1.1	1.1	5379	487	991.971
d	1.0	1.2	5300	271	1040.291
e	1.2	1.0	5399	229	1107.052
f	1.2	1.2	5296	91	1020.944
g	1.0	0.9	5416	620	899.059
h	0.9	1.0	5376	658	973.504
i	0.9	0.9	5404	391	955.999
j	1.0	0.8	5434	125	955.440
k	0.8	1.0	5346	77	1278.195
l	0.8	0.8	5380	15	1405.964

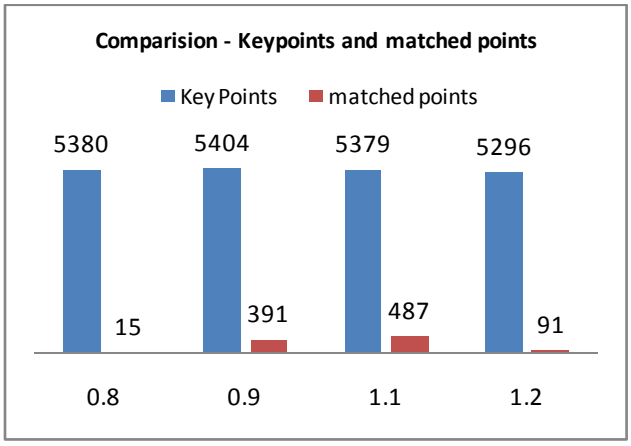

Figure 17. Shows the number of matches decreases when there is scaling.

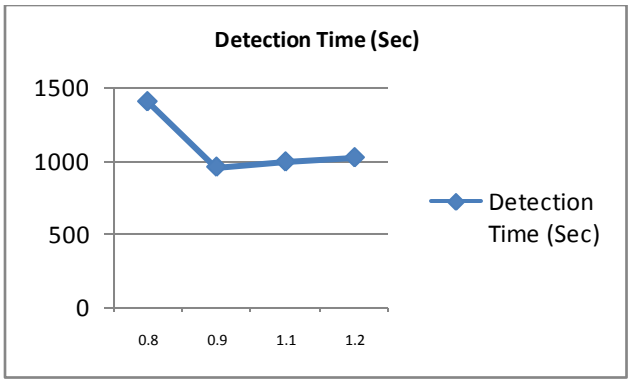

Figure 18. Detection time comparison under different attack for *Acropolis*.

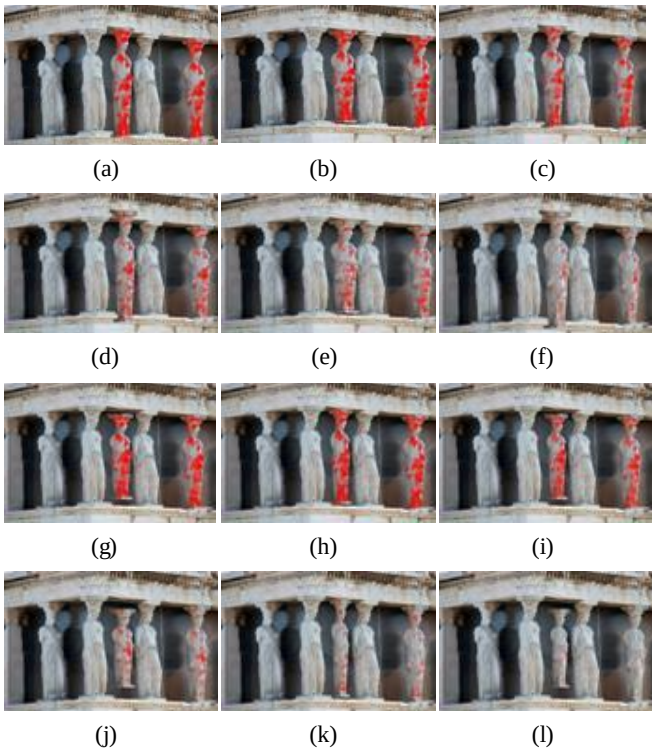

Figure 19. The detection result for various scaling

4. CONCLUSION

A methodology to support image forensic investigation based on Harris Interest Point and SIFT descriptors has been proposed. Given a suspected photo with high resolution and low resolution, the system can reliably detect if certain area has been duplicated. Furthermore, the methodology can effectively detect tampered images which has undergone transformation such as scaling. However, the system is weak in detecting images which has undergone attacks such as rotation and Gaussian noise. In future, we would like to deal with problem such as rotation and Gaussian noise

5. REFERENCES

[1] S. Lyu and H. Farid, "How realistic is photorealistic?" IEEE Transactions on Signal Processing, vol. 53, no. 2, pp. 845–850, 2005.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom, Digital watermarking. San Francisco, CA: Morgan Kaufmann, 2002.

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

[4] H. Farid and S. Lyu, "Higher-order wavelet statistics and their applicationto digital forensics," in Proc. of IEEE CVPR Workshop on StatisticalAnalysis in Computer Vision, Madison, WI, USA, 2003.

[5] S. Bayram, H.T. Sencar, and N. Memon, "A Survey of Copy-MoveForgery Detection Techniques," in Proc. IEEEWestern New York ImageProcessing Workshop, Rochester, NY, USA, October 2008.

[6] 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), pp. 61-65, Sep. 2010

[7] J. Fridrich, D. Soukal, and J. Luk´as, "Detection of copy-move forgery in digital images," in Proc. of DFRWS, 2003.

[8] 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.

[9] A. C. Popescu and H. Farid, "Exposing digital forgeries by detectingtraces of resampling," IEEE Transactions on Signal Processing, vol. 53,no. 2, pp. 758–767, 2005.

[10] S. Bayram, H. Taha Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Proc. of IEEE ICASSP,Washington, DC, USA, 2009.

[11] 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.

[12] S.-J. Ryu, M.-J. Lee, and H.-K. Lee, "Detection of copy-rotate-move forgery using zernike moments," in Proc. of UK, pp. 147-151, 1988.

[13] D. G. Lowe, "Object Recognition from Local Scale-Invariant Features,"in IEEE International Conference on Computer Vision (ICCV),Kerkyra, Greece, 1999, pp. 1150–1517.

[14] H. Bay, T. Tuytelaars, and L. V. Gool, "SURF: Speeded Up Robust Features," in European Conference on Computer Vision (ECCV), Graz, Austria, 2006, pp. 404–417.

[15] J. Matas, O. Chum, M. Urban, and T. Pajdla, "Robust Wide Baseline Stereo from Maximally Stable Extremal Regions," in British Machine Vision Conference (BMVC), vol. 1, London, UK, 2002, pp. 384–393.

[16] K. Mikolajczyk and C. Schmid, "A performance evaluation of local descriptors," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 27, no. 10, pp. 1615–1630, 2005.

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

[18] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgeryin digital images using SIFT algorithm," in Proc. of IEEE Pacific-AsiaWorkshop on Computational Intell. and Industrial Application, 2008.

[19] X. Pan and S. Lyu, "Detecting image region duplication using SIFTfeatures," in Proc. of IEEE ICASSP, Dallas, USA, 2010.

[20] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "Geometric tampering estimation by means of a SIFT-based forensic analysis," in Proc. of IEEE ICASSP, Dallas, USA, 2010.

[21] P. Azad, T. Asfour, and R. Dillmann, "Combining Harris Interest Points and the SIFT Descriptor for Fast Scale-Invariant Object Recognition", In IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), St. Louis, USA,2009.

[22] C. G. Harris and M. J. Stephens, "A Combined Corner and EdgeDetector," in Alvey Vision Conference, Manchester, UK, pp.147–151,1988

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

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