ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
DOI: 10.17485/ijst/2015/v8iS9/54344

Indian Journal of Science and Technology, *Vol 8(S9), 128–139, May 2015*

Image Forgery Detection using Multidimensional Spectral Hashing based Polar Cosine Transform

J. Granty Regina Elwin[1]* and G. Kousalya[2]

[1]CSE, SCAD Institute of Technology, Coimbatore – 641658, Tamil Nadu, India; grantyregina@gmail.com
[2]CSE, Coimbatore Institute of Technology, Coimbatore – 641014, Tamil Nadu, India; kousir@gmail.com

Abstract

The work aims at developing an algorithm for passive detection of copy move forgery in digital images. Accessibility and manipulability of the diverse and sophisticated digital image editing and processing tools has made the integrity of digital images debatable. The sensitivity and importance of the very many applications that revolve around digital images demand absolute authenticity of the digital images. As much simple as image tampering been made by the image editing tools, that much difficult the tampering detection process has become. In this work, a tamper detection method has been proposed that employs polar cosine transform for feature extraction and multi-dimensional spectral hashing for feature matching. The algorithm starts by dividing the image into overlapping patches and then feature vectors are extracted from the patches using Polar Cosine Transform (PCT) and similar patches are identified using multi-dimensional spectral hashing. Finally, post-verification is done to filter out false detection of forged regions. The multidimensional spectral hashing based method uses the outer product Eigen function to improve the performance of similar patch identification. The performance of the algorithm is measured in terms of precision F1 score and recall. Experimental results show that the multi-dimensional spectral hashing based identification of similar patches gives better results compared to some of the existing hashing based techniques. The proposed method proves to be effective in authenticating digital images which are employed in many fields like forensics, medicine, mass media etc.

Keywords: Copy Move Forgery, Feature Extraction, Multidimensional Spectral Hashing, Polar Cosine Transform

1. Introduction

Digital images are easily manipulated using image editing software like Photoshop, Coral Draw and a number of other cost free online applications. Detection of tampered regions in an image is not an easy task, because the forged images look very much similar to original images. Image tampering or image forgery can be done in many ways which include, image enhancement, image splicing, copy-move forgery or a combination of afore stated methods. Image enhancement or image retouching is usually a harmless kind of tampering or editing employed by newspaper, magazine and other mass media editors to improve the aesthetic quality of images. Retouching does not make any significant change on an image but instead, enhances or reduces certain features of an image, like noise, blur, etc. Image splicing is a form of image forgery, wherein parts of image from other image sources are copied and pasted on the original image, resulting in a tampered image. Copy Move forgery or region duplication algorithm is also a form of image splicing in which portions of the same image are copied and pasted elsewhere on the same image with the intent of hiding something or adding something extra to the image. Detection of copy move forgery becomes especially complex when the copied portion has undergone geometrical transformations like scaling, rotation, cropping, etc. before it is pasted. Image tampering detection methods are classified into two types: active and passive. Active detection methods require the images to be protected by watermarks and digital signatures. Image

*Author for correspondence

tampering detection methods that do not depend on any pre-embedded information are classified under Passive tampering detection methods. Passive methods depend on image functions and image statistics and on the subtle changes in the images caused by the tampering.

Passive methods are broadly classified into two categories namely Block based methods and Key-point based methods. In Block based methods, the images are divided into rectangular or circular sub blocks and features are extracted from the sub blocks using Discrete Cosine Transform (DCT), Polar Cosine Transform (PCT), Local Binary Patterns (LBP), Discrete Wavelet Transform (DWT), etc. In key-point based methods, regions of high entropy are identified and SIFT/SURF features are extracted from these regions rather than from sub blocks. Extracted features are then matched and then based on the feature matching, duplicate regions in the image are identified. Some of the copy move forgery detection methods are presented in the literature review. The proposed image forgery detection algorithm shows improved performance compared with existing methods based on spectral hashing. The spectral hashing based detection algorithm starts by dividing the image into overlapping patches. The features are extracted from each patch using Polar Cosine Transform (PCT). The similar patches are identified using spectral hashing techniques. Finally post-verification is done in order to detect the forgery region. The proposed forgery detection algorithm using multidimensional spectral hashing based polar cosine uses the outer product of the Eigen function, so as to improve the algorithm's performance in identifying similar pairs of image regions.

Many passive tampering detection algorithms evolved to battle down the effects of tampering and to ensure authenticity of the images. Some of these methods are discussed in this section. In[1] 2003, it is proposed the first region duplication detection algorithm, which was based on DCT and lexicographic sorting. Passive tampering detection methods involve a diversified range of techniques including DCT[1], DWT[34], Principal Component Analysis PCA[5], DWT and fast Walsh-Hadamard Transform FWHT[33], LBP[17], etc. Detection methods dependent on SVD[6], DWT and Kernel-PCA[7], FMT[8], SIFT[9,10,19], SURF[11,26], blur moment invariants[2], Zernike moments[4], Hu moments[3] etc. were suggested for region duplications where the copied region is further manipulated by rotation, scaling, blurring, compression, variations in luminance etc.

The circular pattern matching and Polar Harmonic Transform (PHT) algorithm could be used for detection of forged regions in images is given in[12]. The dataset used was UCID - Uncompressed Color Image Database which was built with 100 images from the internet. The proposed method was capable of detecting forged regions which had been subjected to affine transforms. The image is first divided into overlapping circular blocks, and Polar Harmonic Transform (PHT) is employed to extract rotation invariant features for each block. Then the features are lexicographically sorted, and block matching is achieved by comparing the Euclidean distances of the feature vectors. The method is not effective in images which had been manipulated by additive noise, blur or JPEG compression.

A tampering detection method which relies on the relation between tampering and sensor pattern noise is proposed in[13]. This method stood out from other such methods because of the fact that their proposed algorithm did not require a recognized image acquisition course or an image database produced by known equipment. Here the image is transferred into a gray scale representation. This image then undergoes a wavelet transform and then Weiner filter is used to obtain the de-noised image. The difference between the original image input and the de-noised image results in the Sensor Pattern Noise (SPN). The feature vector is formed using four different features including, the variance in SPN, image entropy, average energy gradient of the image and SNR between the SPN and the de-noised image. The image is then split into sub-blocks using a non-overlapping sliding window and the feature vector is obtained for each of these sub-blocks. The Euclidean distance between the feature vectors obtained from the sub-blocks and the feature vector obtained from the whole image is used to calculate the similarity between the above mentioned vectors. Accuracy of tampered blocks identification is further compounded by additional morphological methods. The method, though effective in producing acceptable detection rates, even when the image had weathered JPEG compression, additive noise, blurring, rotation and scaling, is capable of detecting copy-move forgery only, if the forgery within the same image.

The region duplication detection algorithm developed which depends on improved Discrete Cosine Transform and exhibits low computational complexity is given in[14]. The profound difference between this method and the other DCT based methods is that; here the quantized

block is characterized by a circle block. The circle block is then divided into a fixed number of parts, for which the feature vectors are calculated. Euclidean distance between adjacent pairs is calculated after lexicographic sorting of the vectors. The actual distance between the similar vectors is also considered before the final call on duplication is made. The method is capable of identification of multiple region duplications and is also robust against blurring and additive noise.

In[15] 2012 it is proposed a computationally complex copy move forgery detection algorithm, which is dependent on circular window expansion and phase correlation. The image is scanned by a circular window and the circular window is then expanded into a normalized rectangular block using bi-linear interpolation. DFT is calculated for these expanded blocks and from this result the phase correlation matrix is obtained, wherein enhanced peak values reflect the similarity in regions. A band limitation procedure is applied to the DFT in order to remove the high frequency components since they do not make any constructive contribution towards the calculation of peak values. The method also identifies copied-rotated - moved regions in the image. The image is scanned by two circular windows and using the peak values the center of identical regions are identified and then a seed filling algorithm is employed to identify the copied region. This method is shown to be accurate in forgery detection even after the forged region had undergone rotation, blurring, JPEG compression, and variations in luminance. The method is not computationally fast and is also not scale invariant.

In[16] 2013, developed a method which relies on the rotation invariant and orthogonal properties of Polar Cosine Transform (PCT), to detect copy move forged regions which had been further manipulated by rotation. The image is subdivided into overlapping circular patches. Feature vectors are extracted for each patch using PCT. Approximate neighbor searching algorithm based on Locality Sensitive hashing (LSH) is used for identifying similar patches. Distance between patches identified as similar by LSH and the neighborhood of such patches are further analyzed, to avoid false detection. Experimental conclusions were drawn that this copy-rotate-move tampering detection method outperforms copy-rotate-move tampering detection method based on Zernike moments. The authors also provide experimental support to show that LSH based similar patch identification is better than the predominantly used lexicographic sorting. The method also reveals a superior level of robustness towards blurring, any added noise, JPEG compression and rotation.

Local Binary Pattern (LBP) based tampering detection method was proposed in[17] and this algorithm can detect copied regions even if the geometry of the forged region is further polluted by noise, blurring, JPEG compression, scaling and rotation in multiples of 90degrees. The image is translated to gray scale and then is sub divided into overlapping blocks. Multi-resolution Local Binary Pattern (MLBP) features are identified for each block by applying different types of LBP operators, after each block has been filtered using adaptive Weiner filter. The feature vectors are put together to form feature matrices; number of feature matrices is equal to the number of LBP operators employed. Feature matrices are lexicographically sorted and k-d tree method is used for determining matching blocks. RANdom SAmple Consensus (RANSAC) algorithm is then used to eliminate false matches. Tampering involving duplicated regions with arbitrary rotation angles cannot be detected by this method.

Scale Invariant Feature Transform (SIFT) is employed in[19] for feature extraction combined with localization based on the J Linkage algorithm for detecting tampering. Sift features are extracted for the image and then these feature vectors are matched using g2NN algorithm. Coordinates of the matched vectors are considered likely candidates for clustering, which are performed using J linkage algorithm. The result of clustering reveals the copied regions. Because the method adopts SIFT features, it is capable of detecting forgeries involving scaling and rotation. The method is successful in detecting multiple duplications and is also able to localize tampered regions with a high degree of precision.

Adaptive Non-Maximal Suppression (ANMS) keypoint selection instead of SIFT features are proposed in[20], because SIFT based methods are not suitable for detecting forgeries in images that have a uniform texture. Keypoints are detected using Harris corner and ANMS is used for selecting the keypoints of interest. For each of these interest points, the DAISY descriptors are evaluated. Keypoints are matched based on The Euclidean distance between the descriptive vectors. Accuracy of matching is enhanced by using 2NN test which relies on the ratio between distance of the first nearest keypoint and the distance to the second nearest one. The method is rotation and scaling invariant and is also robust to JPEG compression and addition of Gaussian noise.

The use of rotation and scaling invariant SURF (Speed up Robust Features) descriptors, for detecting copy move forgery was proposed in[11]. SURF and kd tree algorithm for tampering detection[26]. Keypoints are detected using Hessian Matrix and the SURF descriptors are evaluated for these interest points. The feature descriptors are matched using the kd tree algorithm. Hierarchical Agglomerative Clustering (HAC) along with SURF is used in[35], in which the interest points are identified using Hessian Matrix. Feature descriptors are evaluated by applying SURF. Keypoint matching is done by selecting the nearest neighbors by using the best bin first method. Clustering of matched keypoints is accomplished by HAC. Dimension of SURF descriptor is smaller and so this approach is comparatively faster and the algorithm is also robust to scaling, rotation, luminance variations, JPEG compression, and addition of Gaussian noise.

In general, most of the proposed copy-move forgery detection methods involve two substantial steps: 1. Feature extraction, 2. Feature matching. The accuracy of the matching step may be intensified by additional processing. This paper presents a copy move forgery detection algorithm where the feature extraction is done by Polar Cosine Transform (PCT) and the feature matching is done by Multi-dimensional Spectral hashing.

2. Dataset Details

The dataset is comprised of 100 images, which were collected from various sources. The dataset contains both manually forged images and bench mark images. The manually forged images were created using photo editing software.

3. Proposed Work

In the proposed method, the image is first divided into overlapping patches and feature vectors are extracted from the overlapping patches using Polar Cosine Transform (PCT). Identification of similar patches is done using multidimensional spectral hashing. Finally, post verification is performed to filter out false patches and to detect the forged regions.

The architecture of proposed work is shown in Figure 1.

The image is divided into overlapping patches, and the output of this process is shown in Figure 2. Feature vectors are extracted for each of these patches using polar cosine transform. Polar Cosine Transform is an orthogonal transform which belongs to the family of polar harmonic transform. The PCT contains the following properties. The transform kernel in PCT is orthogonal, and so the features extracted using PCT are more compact than those computed with non-orthogonal kernels. PCT exhibits superior robustness against noise compared to Zernike moments.

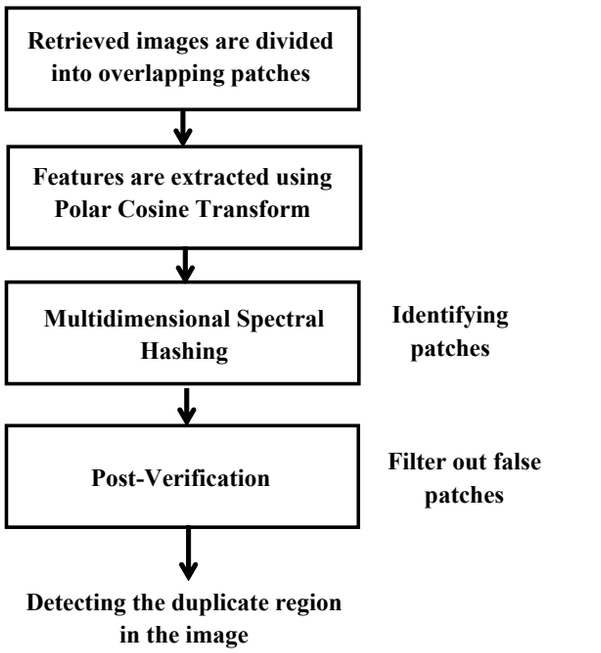

Figure 1. Architecture of forgery detection using multidimensional spectral hashing based Polar Cosine Transform.

The Polar Cosine Transform is defined in polar coordinates. The image represented by Cartesian coordinates, $f(x,y)$ is transformed to polar coordinates, $f(r, \theta)$, where

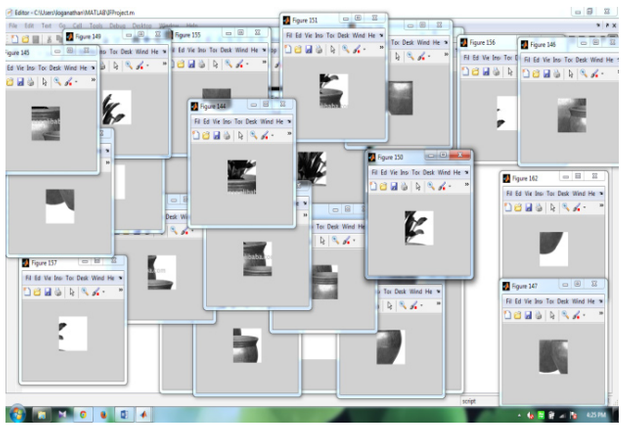

Figure 2. Overlapping patches of image.

(r, θ) are polar coordinates. The center of the image is located in origin, and the pixel coordinates are mapped to the domain of the unit circle. The *f(r, θ)* is expressed as:

$$M_{nl} = \int_{0}^{2\pi}\int_{0}^{1} [H_{nl}(r,\theta)]^{*} f(r,\theta) r dr d\theta$$

Where

- n, [l] = 0,1,2,……,
- $H_{nl}(r, \theta) = \cos(\pi n r^2)e^{il\theta}$ is the PCT kernel, $[.]^{*}$ denotes the complex conjugate operation
- *f(r, θ)* is polar coordinates

$$_{n} = \begin{cases} 1/\pi, n = 0 \\ 2/\pi, n \quad 0 \end{cases}$$

Where n, [l] = 0,1,2,……, $H_{nl}(r, \theta) = \cos(\pi n r^2)e^{il\theta}$ is the PCT kernel, $[.]^{*}$ denotes the complex conjugate operation, and

$$_{n} = \begin{cases} 1/\pi, n = 0 \\ 2/\pi, n \quad 0 \end{cases}$$

In this PCT feature extraction technique, the features are extracted from circular patches with radius R. The PCT coefficients convey different visual information of the patches. For color images, the feature vectors are extracted from different channels and finally concatenated.

4. Multidimensional Spectral Hashing

Multidimensional spectral hashing[36] is an approach for learning binary codes to reconstruct affinity between data points instead of distances. The reconstruction of affinity between data points changes the performance considerably. Literature has it that spectral hashing is better than Binary Reconstructive Embedding and Iterative quantization at small thresholds. The binary code approximation of affinity is given by:

$$W(i,j) = \exp\left(\frac{\left\| x_i \quad x_j \right\|^2}{2\sigma^2} \div \right) \div$$

The approximation of affinity between data points uniformly will approximate the distance in non-uniform quality. It represents the near neighbors appropriately and uses the relation between hamming distance and dot product as,

$$\left\| y_i \quad y_j \right\|^2 = 2k \quad 2y_i^T y_j$$

The optimization problem is formulated as the L2-loss between the inner product and the affinity and it is given by:

$$(Y, \quad) = \arg \min_{y_i \quad \{1,1\}^k, \quad i,j} (Y_i^T \quad y_j \quad W(i,j))^2$$

Here *Y* is an *n*k* matrix and the i^{th} row of *Y* gives the binary code of i^{th} image. The best binary code Y^{*} for a given dataset is equivalent to performing binary matrix factorization of the affinity matrix *W* [3].

Application of multi-dimensional spectral hashing over the extracted feature vectors results in identification of similar patches. Figure 4 shows the patches identified as similar, in binary form.

5. Spectral Relaxation

Relaxing the binary constraint we get a standard matrix factorization problem. The solution is obtained from this problem to find top *k* eigenvectors of *W*. If *U* U^T is the best rank k approximation of the affinity matrix *W*, where *U* is a *n*k* matrix and the top *k* eigenvectors are columns of *U* and is a diagonal matrix with *k* Eigen values. The binary codes are obtained by thresholding the Eigen function. The number of outer product functions may become exponential, but applying a kernel-trick allows to obtain a storage-efficient final Multidimensional Spectral Hashing Algorithm[36].

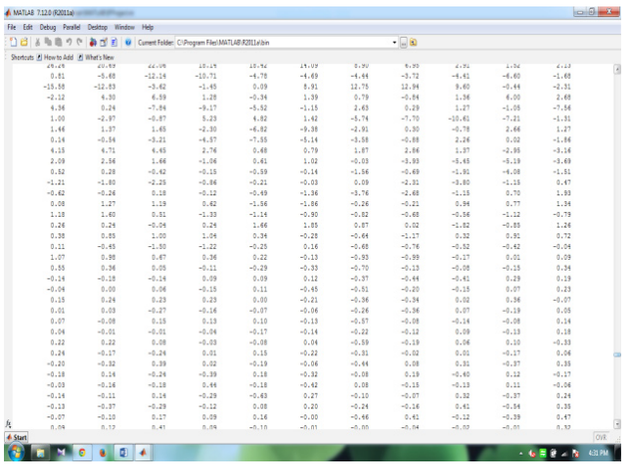

Figure 3. Feature vectors are extracted from overlapping patches using Polar Cosine Transform.

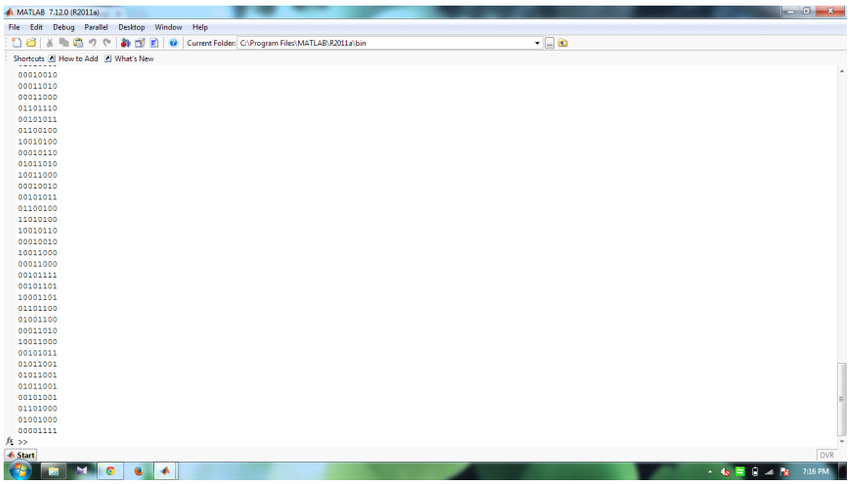

Figure 4. Binary codes of similar patches identified by multi-dimensional spectral hashing.

- Calculate one-dimensional Eigen functions. We denote $\phi_{ij}(x(i))$ by the j^{th} Eigen function of the i^{th} coordinate and λ_{ij} the corresponding Eigen value.

$$\phi_j(x(i)) = \sin\left(\frac{\pi}{2} + \frac{j\pi}{b_i \quad a_i} x(i)\right)$$

$$\lambda_j = e^{-\frac{\sigma^2}{2}\left|\frac{j\pi}{b_i \quad a_i}\right|^2}$$

- Sort λ_{ij} and find a set of k indices (I,J) so that λ_{ij} is maximal.
- Encode each data point x with $y(x) = \text{sign}(\phi_{ij}(x))$ for all $(i, j) \quad (I, J)$.
- The hamming affinity between x_i and x_j is given by

$$H(i,j) = 1 + \quad _d(1 + H(i,j))$$

Where $H_d(i,j) = \quad _{(d,I)\ (I,J)} \lambda_{dI} sign(\phi_{dI}(x_i(d)))$

$$sign(\phi_{dI}(x_j(d)))$$

Input: Feature Vectors.
Output: Similar patches in the form of Binary Code.

Using multidimensional spectral hashing, similar patches of the image are found and from this, the potential pairs of forged regions are identified using the hamming distance between the binary codes. Figure 5 shows the potential pairs of forged regions found by analyzing the hamming distance between the binary codes.

Input: Binary Code.
Output: Potential pair in form of Statistical Information.

6. Post-Verifications

The identified patches are potential copy move forged regions and out of these the false matches are filtered so that the exact tampered regions are identified. A sequence of post-processing operations is performed to filter out any false matches. Any two patches that are identified as similar through multi-dimensional spectral hashing does not necessarily mean that they are forged, because it is natural for the image itself to contain regions that look similar. In order to avoid false identification of forged regions the multi-dimensional spectral hashing output undergoes the following sequence of post-processing operations. The Euclidean distance between the pairs identified through spectral hashing is calculated. The actual forged regions are filtered by comparing the Euclidean distance with the threshold value.

$$\sqrt{(x_1 \quad x_2)^2 + (y_1 \quad y_2)^2} > T_D$$

Here, (x_1, y_1) and (x_2, y_2) represent the potential pair of image patches and T_D is a pre-defined threshold value. Pairs of image patches whose calculated distance is lesser than T_D are not considered as forged regions. Figure 6 shows the patches identified as forged regions, after removing false matches, using the distance criterion.

Input: Potential Pairs identified by multi-dimensional spectral hashing.
Output: Forged regions, after filtering out false patches.

False matches are then eliminated based on the locality of the potential pairs. The clustering of potential pairs

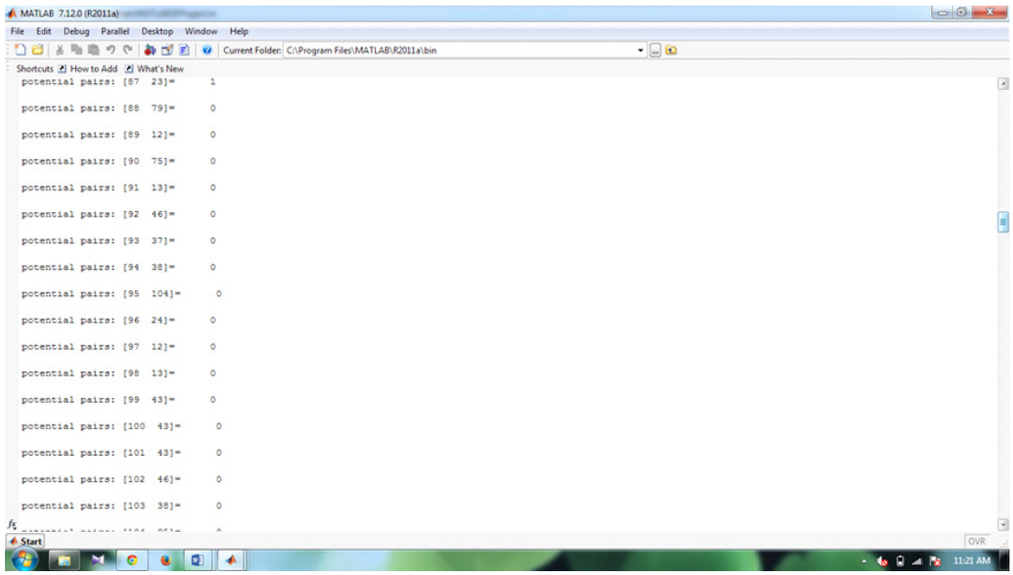

Figure 5. Potential pair of forged patches in form of statistical information.

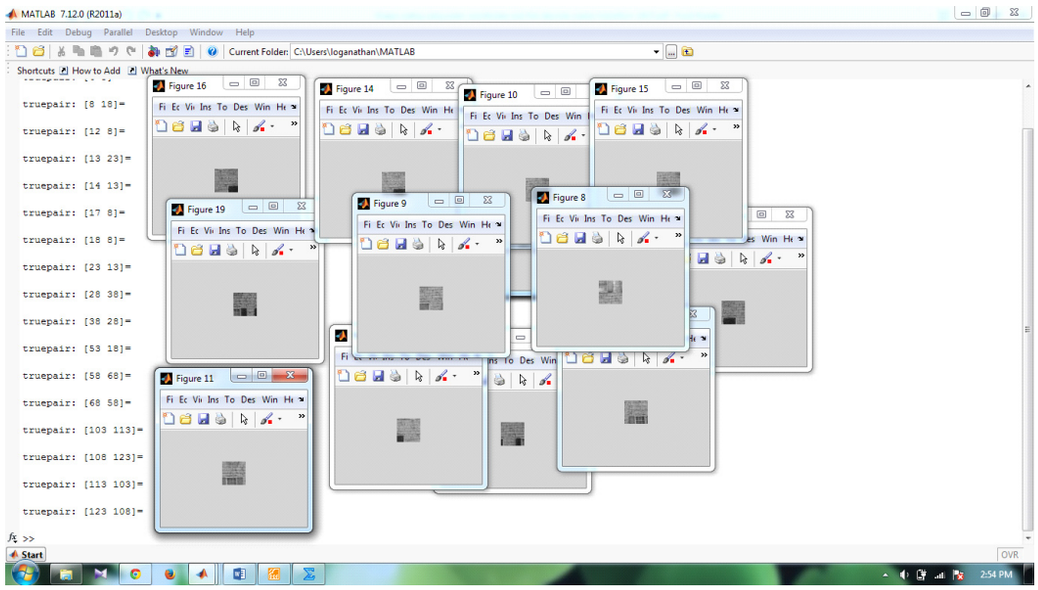

Figure 6. Forged Patches after filtering out false patches, based on the Euclidean distance Criteria.

in two specific neighborhoods is another clue for identification of copy move forged regions. Consider a pair (P1, P2), which is identified by multi-dimensional spectral hashing as a possible forged pair. The eight neighbors of P1, N_8P1 and that of P2 N_8P2 are examined. If any of the eight neighbors of P1 is matched with the corresponding neighbor of P2, then it is called a neighboring pair of (P1, P2). Potential pairs which have more than six neighboring pairs are retained and the rest are filtered as false matches.

Finally, a map showing the forged regions is developed. This is done by creating an all zeros matrix, whose size is equal to the size of the test image. All matrix coordinates that are a part of the pairs which have been identified as

potential forged pairs are set to 1. Morphological opening operation is performed on this matrix which is then multiplied with the test image. This results in a map which clearly depicts the regions which have undergone copy move forgery.

Figures 7 through 10 illustrate the forgery detection results of the proposed algorithm. The algorithm in a nutshell is,

- Image is divided into Overlapping Patches.
- Feature Vectors are extracted using Polar Cosine Transform.
- Similar Patches are identified using Multidimensional Spectral Hashing (MDSH).
- Post Verification is done to filter out the false pairs of similar patches.

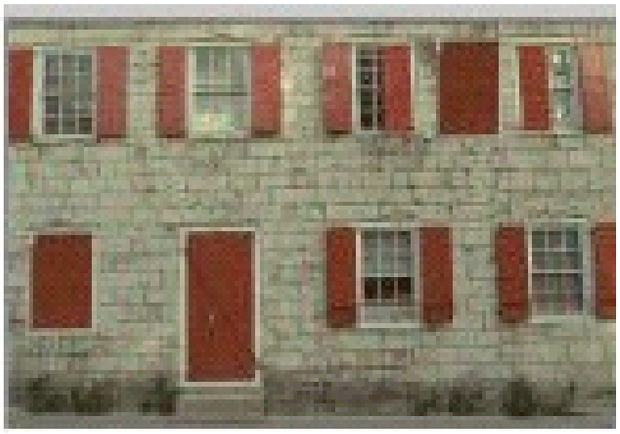

Figure 7. (a) Is input forged image.

Figure 7. (b) Shows the forged regions detected using proposed method.

Figure 8. (a) Is input forged image.

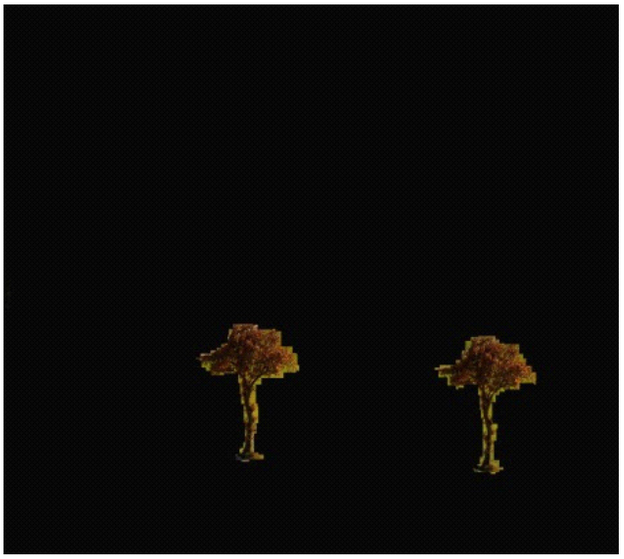

Figure 8. (b) Shows the forged regions detected using proposed method.

7. Result Analysis of Forgery Detection using MDSH based PCT

Precision, Recall and F1 Score are used to evaluate the performance of the proposed approach. The proposed method has shown better performance compared to LSH-PCT and SH-PCT method. The proposed method shows better performance in terms of detecting the forged regions. Among various forgery detection techniques the

Figure 9. (a) Is input forged image.

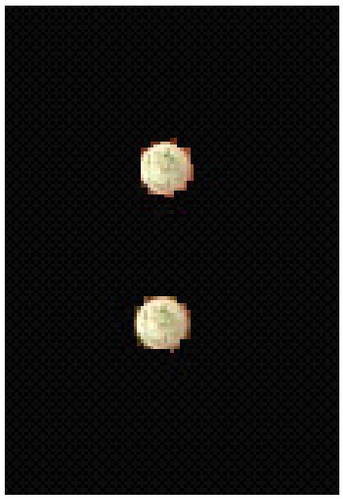

Figure 9. (b) Shows the forged regions detected using proposed method.

Figure 10. (a) Is input forged image.

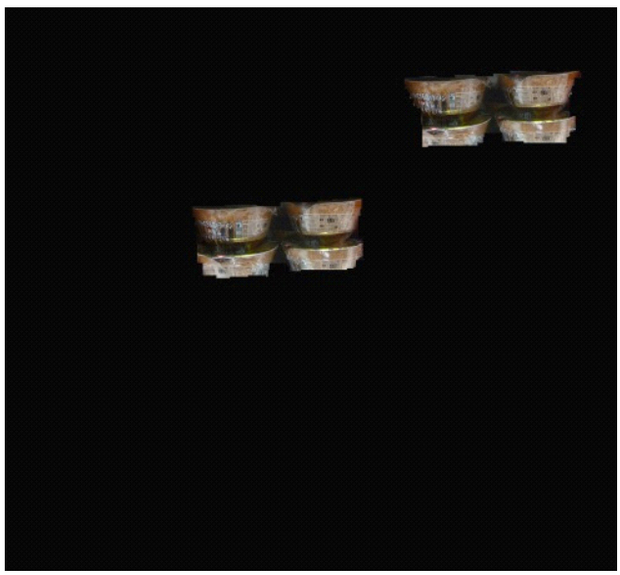

Figure 10. (b) Shows the forged regions detected using proposed method.

proposed method shows high performance in detection of forgery. The precision, recall and F1 score calculated when the proposed approach was applied for detecting copy move forgery compounded with post forgery operations like blur, variance, JPEG compression and rotation is shown in Figures 11 through 14.

The performance of the proposed approach is compared with the performance of LSH-PCT[16] and SH-PCT methods of forgery detection, in detecting copy move forgery, where the forged region is further subjected to blur, variance, JPEG compression and rotation. Table 1 shows the performance of detecting copy-move forgery with single post processing operation and the result is compared to LSH-PCT and SH-PCT methods. The proposed method shows a relatively higher performance in terms of precision, recall and F1 Score.

Similar patches are identified by applying multi-dimensional spectral hashing.

Table 1. Performance comparisons on detecting the copy-move forgery involving single post processing operation

	Proposed Method	SH-PCT	LSH-PCT
Precision	0.99	0.98	0.98
Recall	0.99	1	0.99
F1 Score	0.99	0.99	0.98

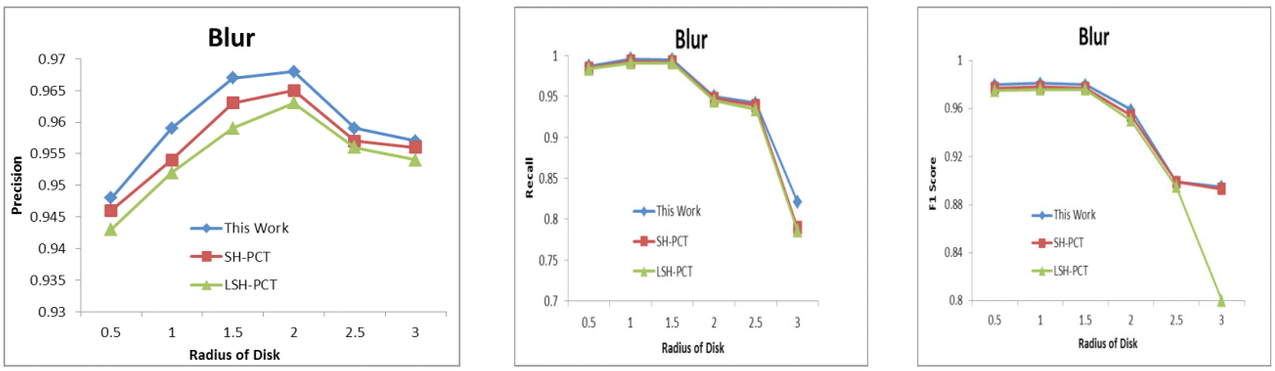

Figure 11. Performance when Blur is applied in forged images.

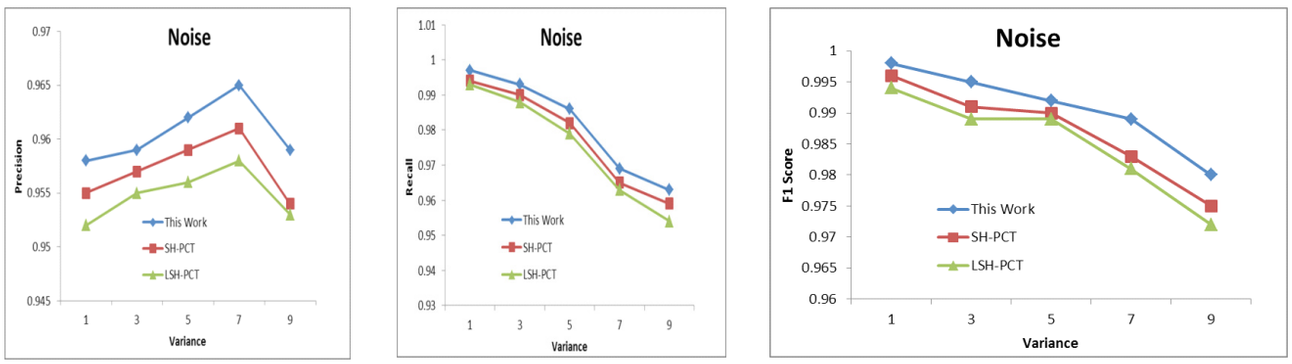

Figure 12. Performance when Noise is applied in forged images.

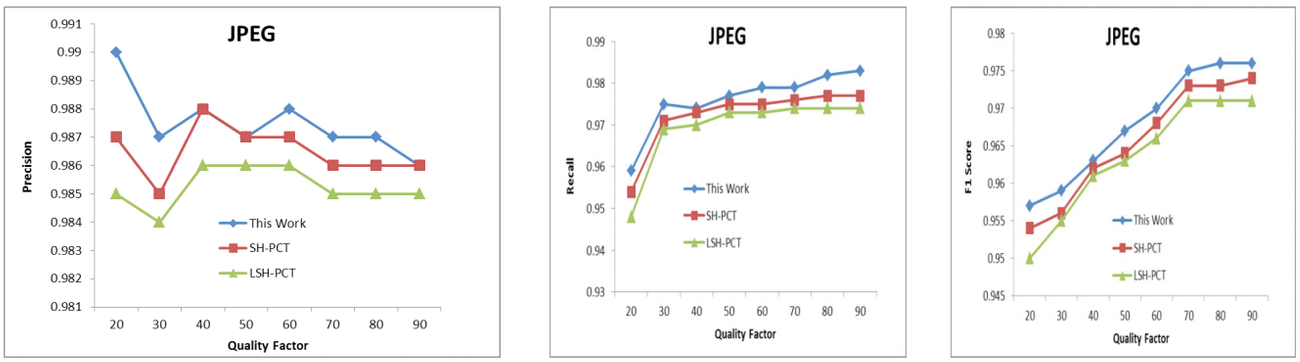

Figure 13. Performance when forged images have undergone JPEG compression.

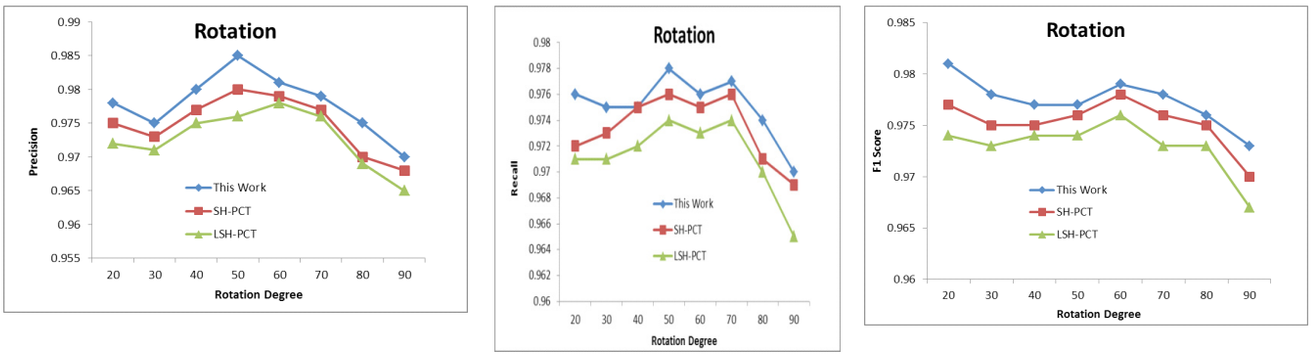

Figure 14. Performance when forged regions have undergone rotation.

8. Conclusion

The proposed forgery detection method is capable of detecting copied regions which had undergone rotational manipulations, since it employs PCT, which is rotation invariant. The multidimensional spectral hashing techniques are used to detect similar patches of the images effectively. The efficiency of the tampering detection algorithm is further compounded by the sequence of post-processing operations performed. The use of the outer product Eigen function to detect the forged regions results in a much more effective detection algorithm, in terms of evaluation metrics like precision, recall and F1 Score compared with the SH-PCT method, in which the outer product Eigen function was excluded.

9. References

1. Fridrich J, Soukal D, Lukas J. Detection of copy-move forgery in digital images. Proceedings of Digital Forensic Research Workshop; 2003.
2. Mahdian B, Saic S. Detection of copy-move forgery using a method based on blur moment invariants. Forensic Sci Int. 2007; 171(2–3):180–9.
3. Liu GJ, Wang JW, Lian SG, Wang ZQ. A passive image authentication scheme for detecting region-duplication forgery with rotation. J Netw Comput Appl. 2011; 34(5):1557–65.
4. Ryu SJ, Lee MJ, Lee HK. Detection of copy-rotate-move forgery using Zernike moments. Proceedings of the 12th Information Hiding Conference; 2010. p. 51–65.
5. Popescu AC, Farid H. Exposing digital forgeries by detecting duplicated image regions. Alberta, Canada: Computer Science, Dartmouth College; 2010. p. 51–65. Report No.: TR2004-515.
6. Kang X, Wei S. Identifying tampered regions using singular value decomposition in digital image forensics. International Conference on Computer Science and Software Engineering; 2008. p. 926–30.
7. Bashar M, Noda K, Ohnishi N, Mori K. Exploring duplicated regions in natural images. IEEE Trans Image Process; 2010 Mar.
8. Bayram S, Sencar H, Memon N. An efficient and robust method for detecting copy-move forgery. IEEE International Conference on Acoustics, Speech, and Signal Processing. 2009 Apr. p. 1053–6.
9. Huang H, Guo W, Zhang Y. Detection of copy-move forgery in digital images using SIFT algorithm. Pacific-Asia Workshop on Computational Intelligence and Industrial Application; 2008 Dec. p. 272–6.
10. Pan X, Lyu S. Region duplication detection using image feature matching. IEEE Transactions on Information Forensics and Security. 2010 Dec; 5(4):857–67.
11. Bo X, Junwen W, Guangjie L, Yuewei D. Image copy-move forgery detection based on SURF. 2011 Third International Conference on Multimedia Information Networking and Security (MINES). 2010 Nov. p. 889–92.
12. Li L, Li S, Zhu H, Wu X. Detecting copy-move forgery under affine transforms for image forensics. Comput Electr Eng. 2014 Aug; 40(6):1951–62.
13. Peng F, Nie Y, Long M. A complete passive blind image copy-move forensics scheme based on compound statistics features. Forensic Sci Int. 2011; 212(1–3):e21–5.
14. Cao Y, Gao T, Fan L, Yang Q. A robust detection algorithm for copy-move forgery in digital images. Forensic Sci Int. 2012; 214(1–3):33–43.
15. Shao H, Yu T, Xu M, Cui W. Image region duplication detection based on circular window expansion and phase correlation. Forensic Sci Int. 2012; 222(1–3):71–82.
16. Li Y. Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching. Forensic Sci Int. 2013; 224(1–3):59–67.

17. Davarzani R, Yaghmaie K, Mozaffari S, Tapak M. Copy-move forgery detection using multiresolution local binary patterns. Forensic Sci Int. 2013; 231(1–3):61–72.
18. Al-Qershi OM, Khoo BE. Passive detection of copy-move forgery in digital images: State-of-the-art. Forensic Sci Int. 2013; 231(1–3):284–95.
19. Amerini I, Ballan L, Caldelli R, Del Bimbo A, Del Tongo L, Serra G. Copy-move forgery detection and localization by means of robust clustering with J-Linkage. Signal Process Image Comm. 2013; 28(6):659–69.
20. Guo J-M, Liu Y-F, Wu Z-J. Duplication forgery detection using improved DAISY descriptor. Expert Syst Appl. 2013; 40(2):707–14.
21. Gomase PG, Wankhade NR. Advanced digital image forgery detection: a review. IOSR-JCE. 2014; 2(16):80–3.
22. Murali S, Chittapur GB, Prabhakara HS, Anami BS. Comparison and analysis of photo image forgery detection techniques. IJCSA. 2012 Dec; 2(6):45–56.
23. Deshpande P, Kanikar P. Pixel based digital image forgery detection techniques. IJERA. 2012 Jun; 2(3):539–43.
24. Kudke SH, Gawande AD. Copy-move attack forgery detection by using SIFT. IJITEE. 2013 Apr; 2(5):221–4.
25. Vimal Raj V, Thomas L. A novel approach for forgery detection of images. IJAIEM. 2013 Aug; 2(8):55–9.
26. Shivakumar BL, Baboo SS. Detection of region duplication forgery in digital images using SURF. IJCSI. 2011 Jul; 8(4):199–205.
27. Sahu G, Kiran U, Sahu F. Forgery detection by extracting features of digital images. International Journal of Research in Advent Technology. 2014 Apr; 2(4):326–8.
28. Ribeiro B, Goncalves I, Santos S, Kovacec A. Deep learning networks for off-line handwritten signature recognition. Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications. Berlin, Heidelberg: Springer; 2011. p. 523–32.
29. Sawant A, Medhekar A, Naik S, Kamble V. Offline method for detection of forged signatures using neural networks. IJEMS. 2014 Jun; 1(6):10–4.
30. Sekhar R, Chithra AS. Recent block-based methods of copy-move forgery detection in digital images. Int J Comput Appl. 2014 Mar; 89(8):28–33.
31. Li P, Wang M, Cheng J, Xu C, Lu H. Spectral hashing with semantically consistent graph for image indexing. IEEE Trans Multimed. 2013 Jan; 15(1):141–52.
32. Loganathan A, Bharathi D. Sparsification of graph laplacian for image indexing using spectral hashing. Proceedings of International Conference on Signal and Speech Processing; 2014 Aug.
33. Yang B, Sun X, Chen X, Zhang J, Li X. An efficient forensic method for copy-move forgery detection based on Dwt-Fwht radioengineering. 2013 Dec; 22(4):1098–105.
34. Muhammad N, Hussain M, Muhammad G, Bebis G. Copy-move forgery detection using dyadic wavelet transform. 8th International Conference on Computer Graphics, Imaging and Visualization; 2011. p. 103–8.
35. Mishra P, Mishra N, Sharma S, Patel R. Region duplication forgery detection technique based on SURF and HAC. The Scientific World Journal. 2013; 2013:267691.
36. Weiss Y, Fergus R, Torralba A. Multidimensional spectral hashing. ECCV'12 Proceedings of the 12th European Conference on Computer Vision; 2012. p. 340–53.