Fast and Robust Copy-Move Forgery Detection Using Wavelet Transforms and SURF

Mohammad Hashmi[1] and Avinash Keskar[2]
[1]Department of Electronics and Communication Engineering, National Institute of Technology Warangal, India
[2]Department of Electronics and Communication Engineering, Visvesvaraya National Institute of Technology Nagpur, India

Abstract: *Most of the images today are stored in digital format. With the advent of digital imagery, tampering of images became easy. The problem has become altogether intensified due to the availability of image tampering softwares. Moreover there exist cameras with different resolutions and encoding techniques. Detecting forgery in such cases becomes a challenging task. Furthermore, the forged image may be compressed or resized which further complicates the problem. This article focuses on blind detection of copy-move forgery using a combination of an invariant feature transform and a wavelet transform. The feature transform employed is Speeded Up Robust Features (SURF) and the wavelet transforms employed are Discrete Wavelet Transform (DWT) and Dyadic Wavelet Transform (DyWT). A comparison between the performances of the two wavelet transforms is presented. The proposed algorithms are different from the previously proposed methods in a way that they are applied on the whole image, rather than after dividing the image in to blocks. A comparative study between the proposed algorithm and the previous block-based methods is presented. From the results obtained, we conclude that these algorithms perform better than their counterparts in terms of accuracy, computational complexity and robustness to various attacks.*

Keywords: *Image forgery; SURF; DWT; DyWT, CMF.*

Received December 10, 2014; accepted June 12, 2016

1. Introduction

In today's world of digital image publishing, images are regularly morphed. Images are tampered to either hide some vital information or to introduce additional information. Forgery detection techniques can broadly be classified as non-blind and blind. Non-blind methods require that some information be embedded in the image in order to detect tampering. Thus, these methods have limited scope. In contrast, blind methods do not require any information to be embedded in the image.

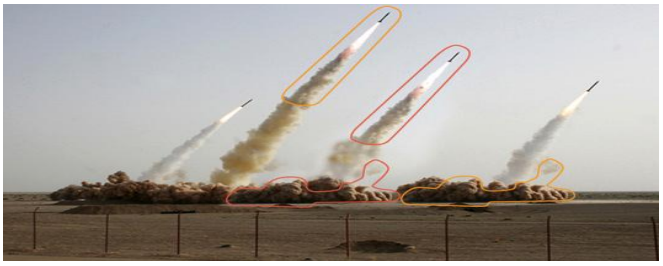


Figure 1. CMF: four missiles shown instead of three.

This article is focused on detection of Copy-Move Forgery (CMF) wherein a patch of an image is copied and pasted onto the same image. A popular example of CMF is shown in Figure 1. It is an image of some missile tests conducted by Iran. The original image contained three missiles. The image was doctored to show four missiles instead of three. Some fundamental principles must be adhered to while designing a CMF detector. First, the detector must not be computationally complex and must detect an authentic image correctly as authentic and a forged image correctly as forged. Second, it must detect an approximate match between small image patches.

2. Existing Detectors

2.1. Block-Based Techniques

The distinctive feature of CMF is that the copied part and the pasted part are similar. Thus, an obvious choice for CMF detection is exhaustive search. Other than being computationally complex, this method is unadvisable since the copied part may be pre-processed by say, Gaussian Blur, before being pasted. However the basis of most of the algorithms is the same, i.e., the similarity between copied and pasted parts. Only blind forgery detection algorithms are discussed herein.

Fridrich *et al.* [6] proposed a block-based approach for detection based on Direct Cosine Transform (DCT). The image is scanned from the upper-left corner with a 16x16 block. For each block, the DCT transform is calculated and the quantized DCT coefficients are stored as a row in a matrix. The rows of the matrix are then lexicographically sorted. The

principle is that matching regions will have similar rows in this matrix. The dimension of the feature vector in this method was sixty-four. This algorithm was obviously computationally complex due to the large size of the feature vector. Popescu and Farid [18] proposed another block-based approach for detection of CMF based on Principal Component Analysis (PCA). This method reduced the feature dimension to thirty-two (half that of the previous method). This method fails when the block sizes are small and the Signal-to-Noise Ratio (SNR) is too low. This technique also fails when the copied region is resampled through rotation or scaling. Cao *et al.* [5] proposed a block based approach for detection of copy-move forgery. The original image is first divided into fixed-size blocks. DCT is then applied to each block. Each transformed block is further represented by a circular block and only four features are extracted from it. Finally, the features are sorted in lexicographical manner and the blocks which are similar will be matched. This algorithm was however computationally complex. It took about 174 seconds for detection of a 1600x1000 image. The performance was also not up to the mark and resulted in many false positives. In fact the only advantage was reduction in feature dimension. The size of the feature vector in this case was four.

Li *et al.* [13] proposed a block-based detection technique based on Local Binary Patterns (LBP). This technique was able to detect the forgery even after the copied region is rotated or flipped before being pasted. The image is first divided in to overlapping circular blocks after low pass filtering it, followed by feature extraction using LBP. Matching feature vectors are detected and thus the image is authenticated. This technique gives reasonable results when the copied region is rotated by 90^o, 180^o, 270^o. The method fails when the copied region is rotated by general angles. A passive method for CMF detection based on DCT and Singular Value Decomposition (SVD) was proposed by Zhao and Guo [21]. This technique was computationally complex since the computation of SVD required a lot of time. Hsu *et al.* [9] proposed a block-based method to detect CMF using Gabor descriptor. Muhammad *et al.* [17] proposed a detection technique based on undecimated Dyadic Wavelet Transform (DyWT). Since DyWT is shift invariant, it is better suited for image analysis than DWT. The input image is decomposed in to LL1 and HH1 sub-bands. LL1 and HH1 sub-bands are divided into overlapping blocks. The principle is that the similarity between copied and moved blocks in LL1 sub-band will be high and in HH1 sub-band will be low due to noise inconsistency in the pasted block.

Bayram *et al.* [3] proposed a block-based technique based on Fourier Mellin Transform (FMT). Further, counting bloom filters, which uses the hashes of the features instead of the features themselves were used in this technique. Qiao *et al.* [19] used Curvelet statistics for detection of copy-move forgery after dividing the image into several overlapping blocks. Li *et al.* [12] devised a sorted neighbourhood method based on DWT and application of SVD. Though the overall process speeds up due to reduction in dimension by DWT, this method is very computationally complex since calculation of SVD takes a lot of time. The method proposed by Ryu *et al.* [20] detects duplicated regions using Zernike moments. Zernike moments have the advantage of being insensitive to noise. In addition, they can provide robust representation of image. Magnitude of Zernike moments can be thought of as the feature representation of the image, which is invariant to rotation. Hence this technique is extremely useful to detect Copy-Rotate-Move (CRM) type of image forgery.

2.2. Key-Point-Based Techniques

Compared to block based techniques, previous investigation of key-point based techniques is quite less. Huang *et al.* [8] proposed a method based on Scale Invariant Feature Transform (SIFT) algorithm for copy-move forgery detection. SIFT descriptors of an image are invariant to rotation, illumination and scaling. SIFT descriptors of the image are first extracted. Descriptors are then matched in order to detect similar patches in the image. Matching is performed using the Best-Bin-First (BBF) search algorithm. Amerini *et al.* [1] proposed a key-point based method for CMF based on SIFT. The key-points and their corresponding SIFT feature descriptors are extracted from the test image. A set of matched points is obtained. Matching key-points are obtained by a generalized version of the 2NN test, referred to as g2NN. For further processing, matched key-points are retained and others are discarded. To reduce the false positives, Hierarchical Agglomerative Clustering (HAC) and geometric transformation estimation was used. The clustering algorithm first assigns every key-point to a cluster and the closest pair of clusters is then merged to form a single cluster. This clustering is repeated until a final merging situation is obtained. Bo *et al.* [4] proposed a CMF detector based on Speeded Up Robust Features (SURF). Though this detector was fast, its robustness to various attacks was not appropriately evaluated previously. The authors seek to address some of the short-comings of previous key-point based techniques in the present article.

3. Theoretical Background

3.1. Wavelet Transforms

Figure 2 shows the process of two dimensional DWT. ‘h’ denotes low pass filter and ‘g’ denotes high pass filter. The LL sub-band contains most of the information and is of primary interest to the authors. In a way, LL sub-band approximates the image. LL

sub-image is divided into four sub-images in the next step and so on [11]. In the proposed algorithm, SURF features are extracted only from the LL part of the image. Computational complexity is naturally reduced since there is lesser data to calculate. Also note that there is down sampling by a factor of two in the process, which reduces the data for further computation. Haar DWT [7] was used by the authors in their implementation. No significant change in results was achieved by modifying the wavelet function. DWT is not optimal for data analysis. To overcome this shortcoming, Mallat and Zhong [15] introduced the DyWT. There is no down-sampling in DyWT like in DWT. Size of the image is reduced at every level by DWT. But by using DyWT, the size of the image remains same.

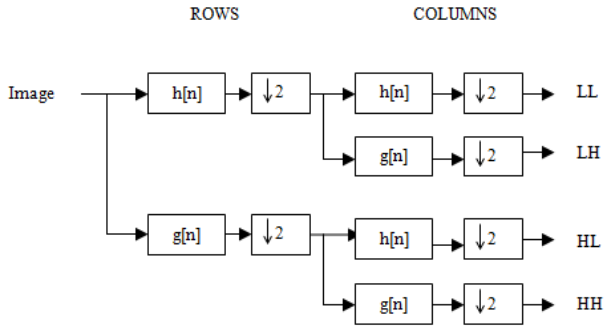


Figure 2. Discrete wavelet transform of an image.

3.2. Speeded Up Robust Features (SURF)

SURF was first presented by Bay *et al.* [2].It is a novel scale- and rotation-invariant interest point detector and descriptor. SURF consists of three major steps. Firstly, physical points of interest in an image are found. These points may be blobs, T-joints or sharp corners etc., Repeatability is a measure of the reliability of the detector to find the same physical interest points under different viewing conditions. The second step consists of formulating descriptor vectors. Descriptor vector consists of nothing but the neighbourhood of every interest point. When the descriptor vector is immune to noise, displacements, rotational variations etc., we say that the detector is robust. Finally, a distance based matching is performed between descriptor vectors of two images. The distance may be Euclidean distance or Mahalanobis distance. SURF is better compared to other detectors and descriptors in terms of repeatability, distinctiveness and robustness.

The primary reason for the popularity of SURF is its lesser computation time. However often in most forensic applications, time complexity is only of limited importance. What matters more is the accuracy. For instance, authenticating an image with an accuracy of 98% may take 3 hours. But it is still better than an image authenticated in 5 minutes with an accuracy of 25%. However SURF does not compromise with performance in return of less computational time. Moreover SURF is not computationally complex. In this article, only an elementary review of the SURF algorithm is presented. For a detailed discussion, refer Bay *et al.* [2].

Juan and Gwun [10] has presented a comprehensive comparison of SIFT, PCA-SIFT and SURF algorithms. The SIFT has a dimension vector of size 128. Since the dimensions in SURF used are sixty-four, the process speeds up. Moreover robustness too increases due to this fact. PCA-SIFT has a 36 dimensional descriptor. In this case, though the matching becomes fast, it becomes less distinctive. GLOH is a variant of SIFT with same number of dimensions, but more distinctive than SIFT [14]. A disadvantage of Gradient Location and Orientation Histogram (GLOH) is that it is very computationally expensive. SURF is thus a clear winner.

4. Proposed Algorithm

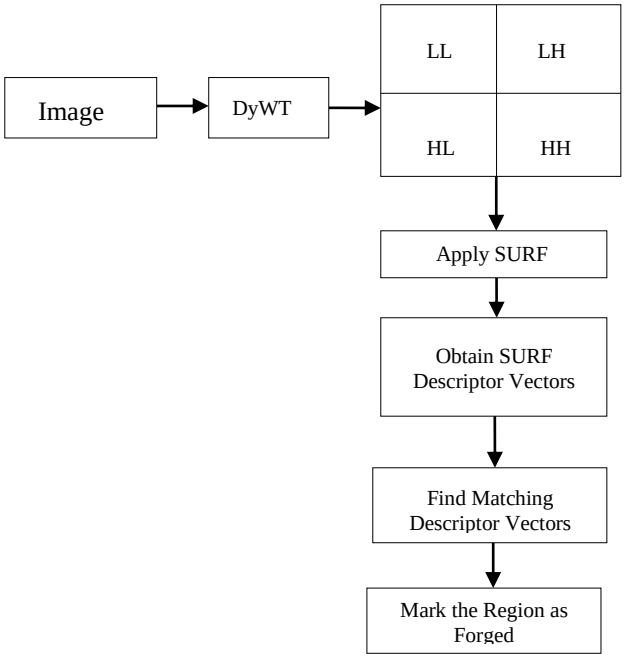


Figure 3. Proposed algorithm.

The proposed technique has been illustrated in Figure 3. The algorithm uses a wavelet transform and an invariant feature transform. First, the test image is converted into grey-scale format if it is in Red, Green, Blue (RGB) format. The technique gave similar results for both RGB and grey-scale images. The image is then transformed in to wavelet domain using either DWT or DyWT (up to level 1). This causes the image to be divided in to four sub-bands. The image is thus split into multi-spectral components. If we use DWT, the size of the image reduces. If DyWT is used, the size of the image remains same. SURF is applied only on the LL part of the image. Descriptor vectors are then sorted in lexicographical order. Matching descriptor vectors are then detected. Matching is performed by the generalized 2NN test (g2NN) as

described by Amerini *et al.* [1]. Thus CMF is detected. The method can detect an image as forged even if the copied part is rotated or scaled and then pasted.

5. Simulation Results and Discussions

5.1. Performance Metrics

$$Accuracy = \frac{TP + TN}{TN + FP + TP + FN} \quad (1)$$

$$FPR = \frac{FP}{FP + TN} \quad (2)$$

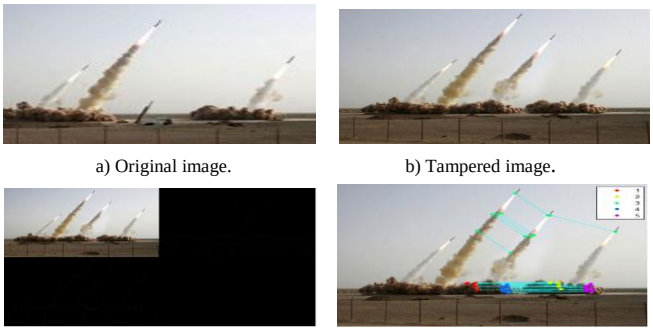
$$Precision = \frac{TP}{TP + FP} \quad (3)$$

$$Recall = \frac{TP}{TP + FN} \quad (4)$$

[TP=True Positive; TN=True Negative; FP=False Positive; FN=False Negative; FPR=False Positive Rate].

5.2. Detection by DWT+SURF

All computations were performed on MATLAB R2012a. An Intel i7 core was used and the system memory was 32 GB. The database used was Media Integration and Communication Centre of the University of Florence, 220 images dataset (MICC-F220) [1]. We also used our own database of about 2000 images. Further, the colored image database released by Institute of Automation, Chinese Academy (CASIA) was used.



a) Original image. b) Tampered image.

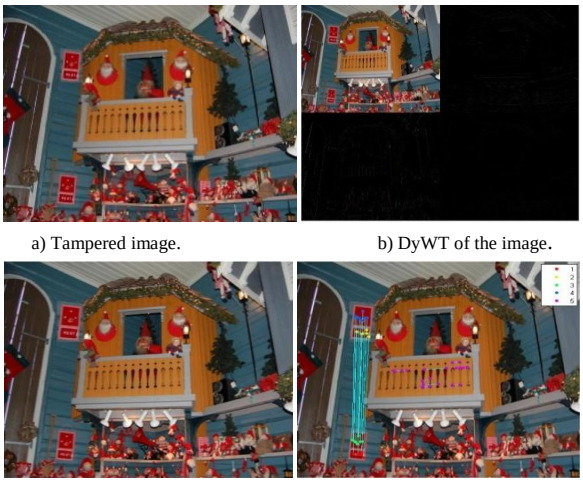
c) DWT of the image. d) Matching of similar features.

Figure 4. Detection process with DWT and SURF.

Figure 4 outlines the detection process with DWT and SURF. Figure 4-a is the original image, with 3 missiles. Figure 4-b is the image tampered with CMF. Figure 4-c shows the image after being transformed by DWT. Figure 4-d shows the matching of similar image patches. For the given image, a total of 302 keypoints were found and 18 matching pairs were detected. The time taken for authentication was 1.567 seconds. When the same image was authenticated using a combination of DWT and SIFT, 325 keypoints were found and 22 matching features were detected. Time required for computation was 2.893 seconds. As we can observe, the performance has negligibly decreased. But the time of computation has decreased by a factor of 1.84.

5.3. Detection by DyWT+SURF

Figure 5 outlines the detection process with DyWT and SURF. Figure 5-a is the tampered image. Figure 5-b shows the transformed image after undergoing transformation by DyWT. Figure 5-c shows only the LL part of the transformed image while Figure 5-d depicts the matching of similar features. For the image shown, 627 key points were found and the number of matching points was 31. The time required for detection was 0.652 seconds. When the same image was tested using DyWT and SIFT, 748 keypoints were found and 46 matching features were detected. Time required for detection was 0.963 seconds. Again in this case, the performance has slightly decreased and computation time has also decreased.



a) Tampered image. b) DyWT of the image.

c) LL part of the image. d) Matching of similar features.

Figure 5. Detection process with DyWT and SURF.

5.4. Performance Under Image Attacks

First, 500 images which had undergone lossy Joint Photographic Expert Group (JPEG) compression were considered in the experiment. The JPEG quality factor ranged from Q=50 to Q=95. For each quality factor, the authors used 50 authentic and 50 forged images. The authentic images used each time are different. The values of precision and recall remain almost similar for different value of quality factor. Precision and recall achieved were 0.791 and 0.804 respectively.

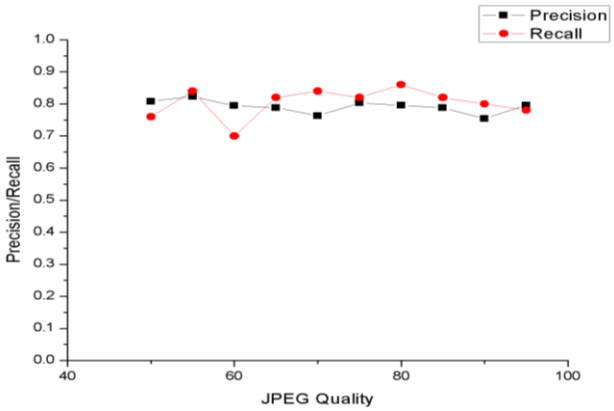


Figure 6. Variation of precision and recall with jpeg quality.

Further, the authors considered 500 images attacked with Additive White Gaussian Noise (AWGN). The SNR of the images ranged from 45 to 65 dB. For each SNR value, they considered 100 authentic and forged images.

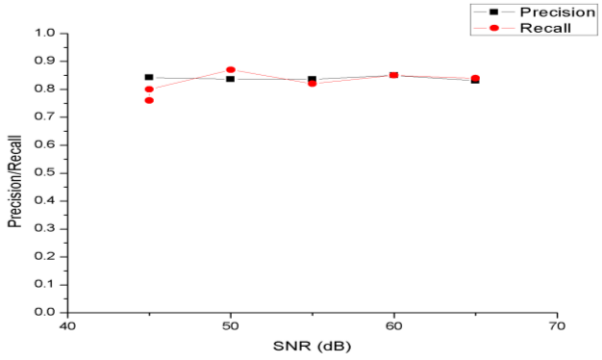


Figure 7. Variation of precision and recall with snr (db).

Further, they considered 500 images filtered by Gaussian Blur. The standard deviation ranged from 0.5 to 5.5. They used 500 authentic and tampered images for each value of standard deviation. Overall the technique achieved a precision of 0.779 and a recall rate of 0.786.

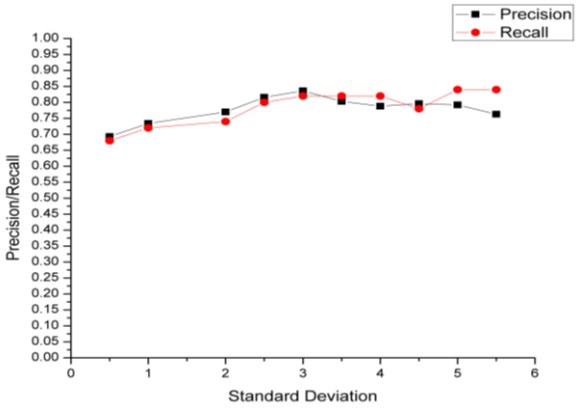


Figure 8. Variation of precision and recall with S.D.

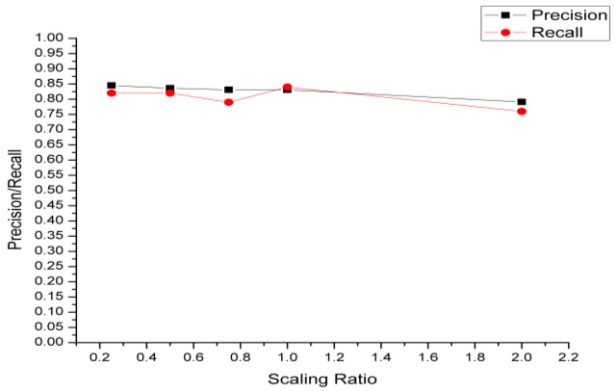


Figure 9. Variation of precision and recall with scaling ratio.

Next, the case of Copy-Scale-Move forgery was considered. In this set of experiments, the copied part was scaled before being pasted in the image. 500 images with different scaling ratios ranging from 0.25 to 2 were considered. Authors used 100 authentic and 100 tampered images for each value of the scaling ratio. Here, the copied part was always a square block of random size. The algorithm achieves a precision of 0.827 and a recall of 0.806.

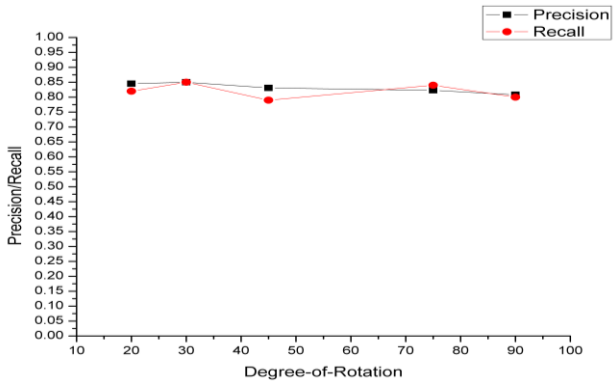


Figure 10. Variation of precision/recall with degree-of-rotation.

Further, they considered 500 images such that the copied part was rotated before being pasted. This is also known as Copy-Rotate-Move (CRM) forgery. The degree of rotation varied from 20° to 90°. They used 100 authentic and tampered images for each value of degree of rotation. The algorithm achieves a precision of 0.831 and a recall rate of 0.82.

Figures 6, 7, 8, 9, and 10 represent the variation of precision with different types of attacks on the test image. The value of precision remains fairly constant for a wide quality of test images. This is an indicator of the robustness of the proposed detector towards various types of image attacks. The variation in recall also remains fairly constant over a wide quality of test images.

5.5. Comparative Study

We used two different wavelet transforms viz. DyWT, DWT and two scale invariant feature transforms- SIFT and SURF. With a combination of these techniques we get four different algorithms. An effort has been made

to compare the performance of these four techniques. The comparison is on the basis of computational complexity. The four techniques were tested on [1] MICC-F220 which comprises of 220 images attacked with CMF. Total time of computation for 220 images was found and average time for one image was thus calculated. Detection time significantly reduces with the application of SURF. It may be noted that the computation time is larger when the wavelet transform used is DyWT than when DWT is used. This is expected since, there is no reduction in size in case of DyWT and there is larger data to compute. The authors have compared detection using SURF, DWT+SURF and DyWT+SURF on the basis of performance metrics. Again, the test dataset used was MICC-F220. Tables 1 and 2 show the comparison.

An effort has been made to compare the proposed technique with both block-based and key-point based techniques. The block-based methods, with which we consider are Fridrich *et al.* [6], Popescu *et al.* [18]. The key-point based techniques with which we consider are Amerini *et al.* [1] and Mishra *et al.* [16]. The performance of the proposed algorithm is a vast improvement over block-based techniques. However its performance is slightly less than other key-point based algorithms. However this fact is negligible in front of the vast improvement in computational complexity. The authors have compared with the existing techniques on the basis of recall and FPR. The FPR of proposed algorithm using DWT+SURF was found to be 0.19 and 0.23 using DyWT+SURF. The TPR was found out to be 0.640 for DWT+SURF and 0.760 for DyWT+SURF. The higher performance of DyWT+SURF is a trade-off at the cost of higher computation time. Table 3 shows the comparative analysis of various performance parameters with previous work.

Table 1. Comparison of computation time.

Technique	Computation time for 220 images (s)	Average computation time (s)
DWT+SIFT	1830	8.3181
DWT+SURF	451	2.05
DyWT+SIFT	22132	100.6
DyWT+SURF	13887	63.122

Table 2. Comparison of performance metrics.

Technique	Precision (p)	Recall (r)
SURF	0.78	0.70
DWT+SURF	0.77	0.64
DyWT+SURF	0.77	0.76

Table 3. Comparison of performance metrics.

Methods	Recall/TPR	FPR
Fridrich *et al.* [6]	0.89	0.84
Pospescu *et al.* [18]	0.87	0.86
Amerini *et al.* [1]	1.00	0.08
Mishra *et al.* [16]	0.7364	0.0364
DWT + SURF	0.640	0.19
DyWT +SURF	0.760	0.23

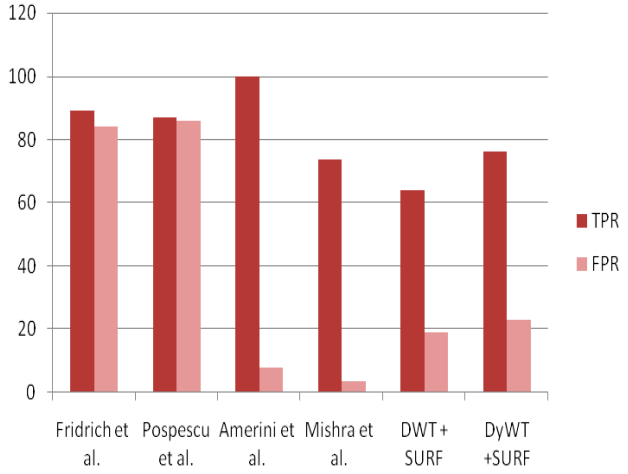


Figure 11. Comparison with existing algorithms.

Figure 11 explains the comparison with existing algorithms with previous algorithms. The proposed detector has marked advantages over the detector of Mishra *et al.* [16]. The proposed algorithm (DyWT+SURF) has higher recall than the recall of the detector of Mishra *et al.* [16]. This implies that the ability of the proposed algorithm to detect a forged image as forged is higher than the algorithm of Mishra *et al.* [16]. Mishra *et al.* [16] perform the feature matching in spatial domain, whereas feature matching in the wavelet domain is the key feature of the proposed detector. Further, the authors find no difference in the algorithm of Mishra *et al.* [16] and the algorithm of Amerini *et al.* [1], except for the replacement of SIFT by SURF. Though Mishra *et al.* claim that their detector is robust to various image attacks; they do not provide any basis for this claim in their article. In contrast, the authors of this paper investigated the variation of precision and recall of the detector after exposing the image to image attacks. Their claim of robustness of their algorithm is based on the fact that the precision and recall of the detector remain reasonably unchanged even after exposing the image to various image attacks. Further, Mishra *et al.* [16] do not provide any conclusive reason for robustness of their detector. In contrast, the authors of this paper attribute the robustness of their detector to feature matching being performed in the wavelet domain rather than in the spatial domain. In fact, the authors conclude that the proposed detector is more robust than the detectors of Mishra *et al.* [16] or Amerini *et al.* [1], since both these detectors perform feature matching in the spatial domain. Further, Mishra *et al.* [16] do not investigate the computational complexity of their detector in detail. In contrast, the authors of the present paper investigate the computational complexity of the proposed detector on various platforms, using various operating systems. Moreover, the proposed detector (DWT+SURF) takes an average time of 2.05 seconds to authenticate the image, whereas the detector of Mishra *et al.* [16] takes 2.85 seconds to authenticate an image. This reduction

in computational complexity is attributed to the fact that in the proposed algorithm, SURF is applied to only the LL part of the image, rather than the whole image. In conclusion, the proposed detector is more robust and computationally less expensive than the detector proposed by Mishra *et al.* [16].

7. Conclusions

The authors examined the existing block based and key-point based techniques to detect CMF. It was found that most of the techniques were either computationally complex or were not robust enough to image attacks. A need was felt to develop a technique for CMF detection which was robust, fast and computationally inexpensive. The proposed detector is fast due to low feature vector length of SURF compared to SIFT. Furthermore, SURF is robust to scaling and rotation. Though some articles have previously used SURF in CMF detection, its role in the process was not appropriately addressed. Due to the use of wavelet transforms, the algorithm is robust to external attacks like AWGN, JPEG compression, Gaussian blurring etc. Haar DWT and DyWT were the wavelet transforms used in the implementation of the detector. No significant change in results was noticed by changing the wavelet function. It was found that when DyWT is used, the number of keypoints and matching descriptor vectors increases. Hence, detector accuracy increases slightly. However this is compensated by higher computational time required by DyWT+SURF. The precision of the CMF detector remains fairly constant over a wide quality of test images, thus proving its robustness. As said before, in the field of digital image forensics, accuracy is more important than computational complexity. However, the same cannot be said about digital video forensics. The true importance of the proposed work would be fully realized when it is modified to detect video forgeries. Along with this, the authors would like to observe the performance of this CMF detector on embedded platforms. Further, the authors wish to check the performance of other invariant feature transforms such as PCA-SIFT when used in conjugation with wavelet transforms.

References

[1] Amerini I., Ballan L., Caldelli R., Del Bimbo A., and Serra G., "A Sift-Based Forensic Method For Copy-Move Attack Detection and Transformation Recovery," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099-1110, 2011.

[2] Bay H., Tuytelaars T., and Van Gool L., "Surf: Speeded up Robust Features," *in Proceedings of European Conference on Computer Vision*, Graz, pp. 404-417, 2006.

[3] Bayram S., Sencar H., and Memon N., "An Efficient and Robust Method for Detecting Copy-Move Forgery," *in Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, Taipei, pp. 1053-1056, 2009.

[4] Bo X., Junwen W., Guangjie L., and Yuewei D., "Image Copy-Move Forgery Detection Based on SURF," *in Proceedings of IEEE International Conference on Multimedia Information Networking and Security*, Nanjing, pp. 889-892, 2010.

[5] Cao Y., Gao T., Fan L., and Yang Q., "A Robust Detection Algorithm for Copy-Move Forgery in Digital Images," *Forensic Science International*, vol. 214, no. 1, pp. 33-43, 2012.

[6] Fridrich J., Soukal D., and Lukáš J., "Detection of Copy-Move Forgery in Digital Images," *in Proceedings of Digital Forensic Research Workshop*, Cleveland, pp. 1-8, 2003.

[7] Haar A., "Zur Theorie Der Orthogonalen Funktionensysteme," *Mathematische Annalen*, vol. 69, no. 3, pp. 331-371, 1910.

[8] Huang H., Guo W., and Zhang Y., "Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm," *in Proceedings of IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, Wuhan, pp. 272-276, 2008.

[9] Hsu H. and Wang M., "Detection of Copy-Move Forgery Image Using Gabor Descriptor," *in Proceedings of IEEE International Conference on Anti-Counterfeiting, Security and Identification*, Taipei, pp. 1-4, 2012.

[10] Juan L. and Gwun O., "A Comparison of Sift, PCA-SIFT and SURF," *International Journal of Image Processing*, vol. 3, no. 4, pp. 143-152, 2009.

[11] Khalifa O., "Wavelet Coding Design for Image Data Compression," *The International Arab Journal of Information Technology*, vol. 2, no. 2, pp. 118-127, 2005.

[12] Li G., Wu Q., Tu D., and Sun S., "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, pp. 1750-1753, 2007.

[13] Li L., Li S., Zhu H., Chu S., Roddick J., and Pan J., "An Efficient Scheme for Detecting Copy-Move Forged Images by Local Binary Patterns," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 1, pp. 46-56, 2013.

[14] Liu T., Kim S., Lim S., and Lee H., "Selection of Distinctive Sift Feature Based on Its Distribution on Feature Space and Local Classifier for Face Recognition," *The International Arab Journal of*

Information Technology, vol. 10, no. 1, pp. 95-101, 2013.

[15] Mallat S. and Zhong S., "Characterization of Signals from Multiscale Edges," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 14, no. 7, pp. 710-732, 1992.

[16] Mishra P., Mishra N., Sharma S., and Patel R., "Region Duplication Forgery Detection Technique Based on SURF and HAC," *The Scientific World Journal*, vol. 2013, no. 6, pp. 8, 2013.

[17] Muhammad G., Hussain M., and Bebis G., "Passive Copy Move Image Forgery Detection Using Undecimated Dyadic Wavelet Transform," *Digital Investigation*, vol. 9, no. 1, pp. 49-57, 2012.

[18] Popescu A. and Farid H., "Exposing Digital Forgeries By Detecting Duplicated Image Regions," Technical Report TR2004-515, Dartmouth College, 2004.

[19] Qiao M., Sung A., Liu Q., and Ribeiro B., "A Novel Approach for Detection of Copy-Move Forgery," *in Proceedings of 5th International Conference on Advanced Engineering Computing and Applications in Sciences*, Lisbon, pp. 44-47, 2011.

[20] Ryu S., Lee M., and Lee H., "Detection of Copy-Rotate-Move Forgery Using Zernike Moments," *in Proceedings of International Workshop on Information Hiding*, Calgary, pp. 51-65, 2010.

[21] Zhao J. and Guo J., "Passive Forensics for Copy-Move Image Forgery Using A Method Based on DCT and SVD," *Forensic Science International*, vol. 233, no. 1, pp.158-166, 2013.

Mohammad Hashmi the author completed his B.E. from VNIT, Nagpur in 1979 and received gold medal for the same. He completed his M.E. from IISc, Bangalore in1983, receiving the gold medal again. He also completed his Ph.D. from VNIT Nagpur in1997.The author is a member of IAENG. He has 26 years of teaching experience and 7 years of industrial experience. He is currently a Professor at Department of Electronics Engineering, VNIT Nagpur. His current research interests include Computer Vision, Soft Computing, and Fuzzy Logic etc. Dr.Keskar is a senior member of IEEE, FIETE, LMISTE, FIE.

Avinash Keskar the author received his B.E in Electronics & Communication Engineering from R.G.P.V Bhopal University in 2007. He obtained his M.E. in Digital Techniques & Instrumentation in 2010 from R.G.P.V Bhopal University. He received Ph.D. at VNIT Nagpur under the supervision of Dr.A.G.Keskar. He has published up to 50 papers in National/International Conferences/ Journals. He has a teaching experience of 7 years. He is currently an Assistant professor at Department of Electronics and Communication Engineering, National Institute of Technology, Warangal. His current research interests are Image Processing, Internet of Things, Embedded Systems, Biomedical Signal Processing, Computer Vision, Circuit Design, and Digital IC Design etc. Mr. Mohammad F. Hashmi is a member of IEEE, ISTE, and IAENG.