I.J. Modern Education and Computer Science, **2016, 12, 56-63**
Published Online December 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2016.12.08

Improvement in Copy -Move Forgery Detection Using Hybrid Approach

Gurmeet Kaur Saini
CGC Landran,Computer Science Department, Mohali,India
Email: gurmeetsaini02@gmail.com

Manish Mahajan
CGC Landran,Computer Science Department, Mohali,India
Email: cgccoe.hodcse@gmail.com

Abstract—In this present digital world, digital pictures and videos are the main sources of information. However, these carriers of information can be easily tampered by using softwares such as Adobe photoshop, GIMP etc. Thus, the issue of verification of authenticity and integrity of digital images becomes necessary. Copy Move Forgery is a popular type of forgery that is commonly used for the manipulation of digital images. In this, a region of digital image is copied and then pasted to another location with in the same image with intension to make an object disappear from an image by covering it with small block copied from another part of the same image. There are several post processing operations that are applied by manipulators to obstruct the forgery detection techniques. Thus, for aforementioned problem, we in this paper proposed a method which is a combination of SIFT and SURF algorithms. In this firstly image is split in to sub-parts by DWT method and then SIFT and SURF are applied to actual components of image one by one. After this, features extracted by both methods are matched to locate the forged part in the image. The experiment shows that the proposed method is more efficient and provides better results than applying SIFT and SURF alone.

Index Terms—Copy Move Forgery, SURF(Speed Up Robust Features), SIFT (Scale Invariant Feature Transform), DWT(Discrete Wavelet Transform).

I. INTRODUCTION

Because of recent advancement in the imaging technology, it is very easy to preserve an important information in the form of digital images and this digital information is being used for multiple purposes like electronic media, scientific discoveries etc. due to development of editing softwares, even a novice person can tamper an image with an ease. As a result, the verification of authentication and integrity of digital images is becoming important.

Digital image forgery detection has been growing very fast in the recent years as research domain [5]. Mainly, the digital image forgery is classified in to two categories: copy move forgery or cloning and splicing [6]. In copy move forgery, some content of image is copied and pasted somewhere else in the same image to hide the important information as shown in Fig. 1. In image splicing, a content of image is replaced by the content of some another image as shown in Fig. 2.

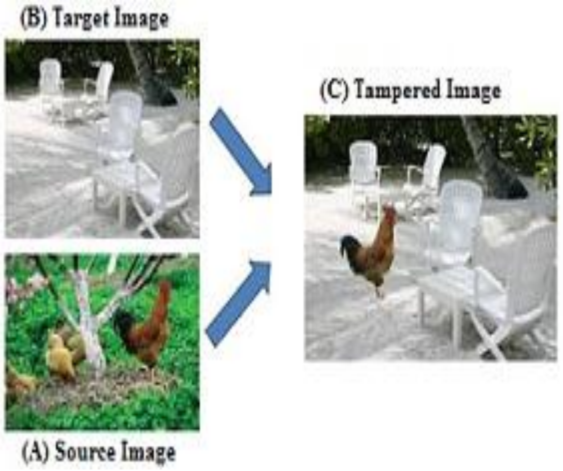
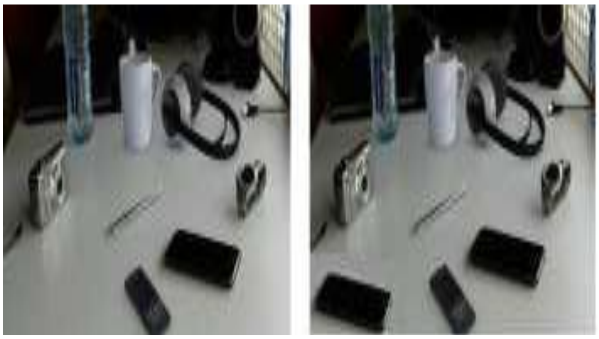


Fig.1. An example of image splicing forgery



(A) Original image (B) Forged Image

Fig.2. An example of copy-move forgery

Digital Image Forgery detection techniques are classified in to two categories: active and passive as shown below in Fig.3. In active method, where some embedded digital information is required about the original image to detect the tampering. For example: Digital watermarking. In passive method, there is no prior information about the original image is required to detect the forgery. For example: Copy-Move Forgery.

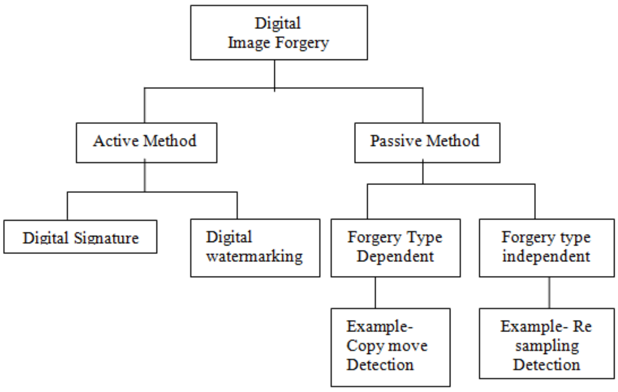


Fig.3. Types of Forgery

Currently our focus is on copy move forgery detection because the task of forgery detection becomes difficult in this case. This is because when the content of image are copied and pasted on that very image they have similar characteristics of that of original image. For this DWT is applied on the image to partition the image in to different parts. After image decomposition, Surf and Sift algorithm will apply to extract image features and then matching of features that are extracted by SIFT and SURF is done to detect the forgery in the image.

The remaining paper is organized as follows: section II explains a previous work related to copy-move forgery detection. Section III completely explain the proposed method. Section IV contains the result analysis of the proposed method on sample images. Section V concludes the work done and scope for future enhancements in the proposed work.

II. Related Works

The literature review has been conducted in detail over the adequate number of techniques to know their advantages and shortcomings. The related work has been defined as following:

Christlein, V. et al.[1] aims to perform best in various post-processing scenarios. The focus is to evaluate the performance of previously proposed feature sets by casting existing algorithms in a common pipeline. In this paper 15 most prominent feature sets are examined and analyzed the detection performance on a per-image basis and on a per-pixel basis.

Amerini, I., et al.[2] proposed a methodology based on on scale invariant features transform. This method allows us to detect whether copy-move attack has occurred and also how to recover the geometric transformation used to perform cloning. This method deals with multiple cloning.

Bo, X. et al. [3] proposed a method based on the SURF (Speed up Robust Features) descriptors, which are invariant to rotation, scaling etc. As the digital images can be manipulated easily without leaving any obvious visual clues. To overcome this problem, this method is proposed and also it is valid in detecting the image region duplication and quite robust to additive noise and blurring.

Hashmi, M. F. et al.[4] developed an algorithm of image-tamper detection based on the DWT which is used to dimension reduction and increases the accuracy of results. Firstly, DWT is applied on the image to divide the image in to sub-parts. After this, SURF is applied on the actual part and then search for the similarities between descriptor vectors to conclude whether the image is forged or not.

Sridevi, M.et al. [6] surveys different types of image forgeries. This survey has been done on existing forgery detection techniques for images and also highlights some copy – move forgery detection methods based on their complexity.

Jaberi, M. et al.[8] propose algorithm based on set of keypoint-based features, called MIFT, which contains the properties of SIFT features. This approach has been evaluated and compared with different competitive approaches through a comprehensive set of experiments using a large dataset of real images.

Muhammad, N. et al. [9] proposed an efficient passive methodology for copy-move forgery detection which is based on image partition and similarity detection using DyWT. Copied regions and pasted regions are structurally similar and DyWT is used to detect this type of structural similarity.

Cao, G. et al.[10] we propose two novel methods to detect the contrast enhancement involved manipulations in digital images. Firstly, detect global contrast enhancement applied to the JPEG-compressed images. Secondly, identify the composite image created by enforcing contrast adjustment on either one or both source regions. The consistency between regions is checked for whether the image is forged or not.

III. Experimental Design

In this paper, the algorithms namely: SURF, and SIFT are used for detection of copy-move image forgery which are discussed below:

A. Surf

SURF (**Speeded Up Robust Features)** is a local feature detector and descriptor that can be used for different tasks such as object recognition or classification or 3D reconstruction. It is partly inspired by the scale-invariant feature transform (SIFT) descriptor.

This method is computationally very fast due to the use of integral images. In SURF, Key-point detection and descriptors are formed as explained below:

(i) Interest Point Detection

For interest point detection SURF uses a basic Hessian –Matrix with integral images which reduces the computational time.

Consider a point X=(x,y) in an image I, the hessian matrix H(X,σ) in X at scale σ is calculated as shown in equation 1:

$$H(X,\sigma)=\begin{bmatrix} L_{xx}(X,\sigma) & L_{xy}(X,\sigma) \\ L_{xy}(X,\sigma) & L_{yy}(X,\sigma) \end{bmatrix} \quad (1)$$

In the above matrix, $L_{xx}(X,\sigma)$ denotes the convolution of the Gaussian second order derivative with the image I at point.

(ii) Interest point description

For interest point description, Firstly SURF creates a circular region around the interest points that are detected to assign them a unique orientation. This is usually done to achieve invariance to rotation. Then for descriptor extraction, a square region is constructed around the interest points and centered to divide it in to 4*4 sub-regions. For each of these Haar-wavelet responses horizontal d_x and vertical d_y directions that are summed over each sub-region. For each sub-region, Feature vector is calculated as:

$$V= (\sum d_{x,} \sum d_{y,} \sum | d_x | , \sum | d_y |)$$

Where $| d_x |$, $| d_y |$ are sum of absolute values of responses. The working of SURF algorithm is shown in flow chart below:

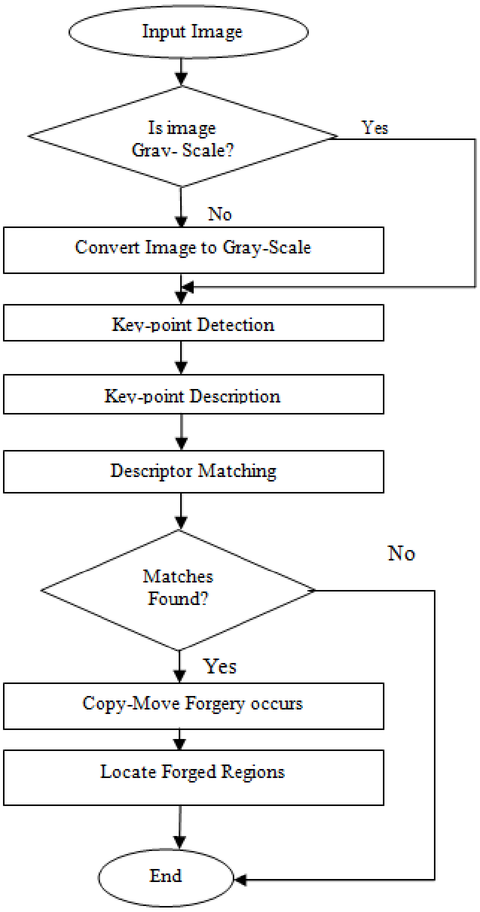


Fig.4. Flow chart of SURF Algorithm

In order to determine copy move forgery, following steps are performed:

Step1: Given Forged Image.

Step 2: Check whether the given image is a gray-scale image or not. If it is not in Gray-scale, first convert it in to Gray-scale.

Step 3: Then SURF method is used to perform the feature extraction and description vectors.

Step 4: After this matching is done to locate the forged part in digital image.

Step 5: Then Key-points are constructed and marked on the digital image.

B. Sift

Scale-invariant feature transform (or SIFT) is an algorithm in computer vision to detect and describe local features in images.

SIFT is used to provide the interesting points on the object that can be extracted to provide a "feature description" of the object. This description can be extracted from the training image, and then it can be used to identify the object . To perform reliable recognition, it is necessary that the features that are extracted from the training image should be detectable even under situations like changes in image scale, noise etc. The working of SIFT algorithm is shown in flow chart below:

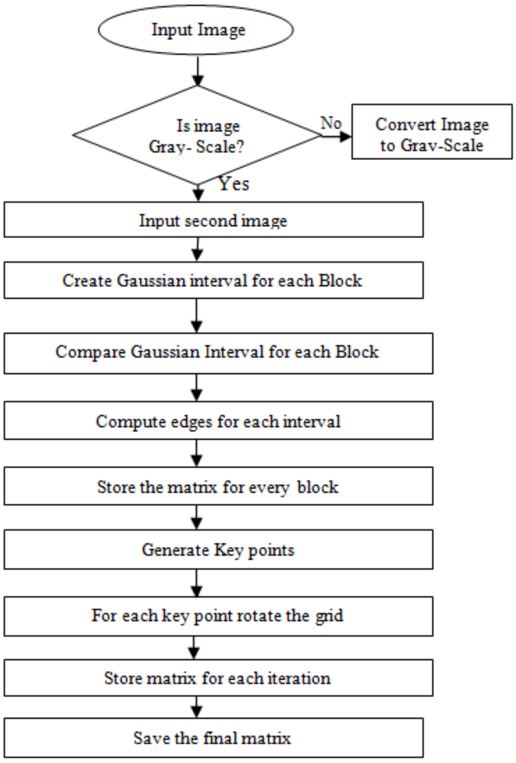

Input Image
Is image Gray- Scale?
No
Convert Image to Gray-Scale
Yes
Input second image
Create Gaussian interval for each Block
Compare Gaussian Interval for each Block
Compute edges for each interval
Store the matrix for every block
Generate Key points
For each key point rotate the grid
Store matrix for each iteration
Save the final matrix

Fig.5. Flow chart of SIFT Algorithm

In order to determine copy move forgery, following steps are performed:

Step 1: First of all discrete wavelet transform is applied on to the given image to decompose the image in to four parts LL, LH, HL, HH.

Step 2: Most of the information is contained in LL part (actual as shown in flow chart below), so we apply SIFT feature extraction on LL part.

Step 3: This will give feature extraction of interest key points.

Step 4: Matching is done between these feature extractions to mark the forged regions.

C. Combined Work of Sift and Surf

To propose a new technique for copy-move forgery detection, at first ,image will be transformed into wavelet domain using DWT and SIFT is applied on the transformed image to obtain the features. For second level feature transformation SURF will be applied. As wavelet produces multispectral components, features are more predominant. After obtaining interest point feature descriptor we will go for finding matching between these feature descriptors to conclude either tampering is done with the given image or not at the post processing level. Our works confirm that combination of SIFT and SURF features are an optimal solution because of their high computational efficiency and robust performance.

The working of proposed system is shown in the flow chart below:

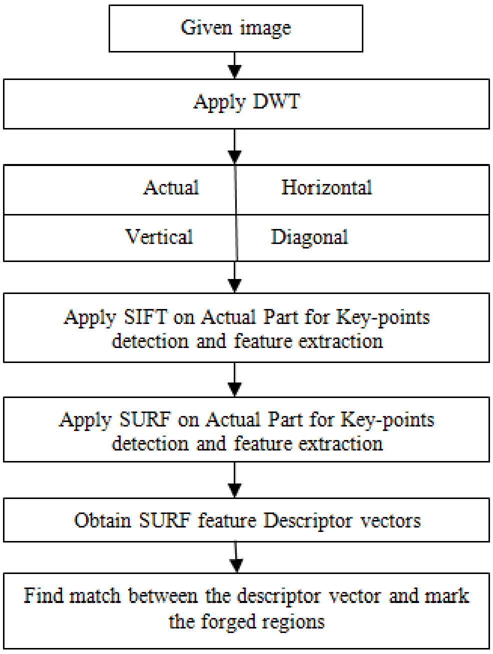

Given image
Apply DWT
Actual
Horizontal
Vertical
Diagonal
Apply SIFT on Actual Part for Key-points detection and feature extraction
Apply SURF on Actual Part for Key-points detection and feature extraction
Obtain SURF feature Descriptor vectors
Find match between the descriptor vector and mark the forged regions

Fig.6. Flow chart of proposed Algorithm

In order to determine copy-move forgery, following steps are performed:

Step 1: Obtain the non-matching key points for SIFT Algorithm.

Step 2: Obtain the non-matching key-points for SURF Algorithm

Step 3: Apply SVM classifier to remove key-points for same pixel values.

Step 4: Store all key-points in a matrix.

Step 5: Mark all the key-points on the image.

IV. Result Analysis

The proposed method is implemented using MATLAB 2015 and tested on an Intel Core i3 with 4GB of RAM running Windows 7. This platform should be considered as the minimum hardware requirement since the image forgery detection algorithms could have been modified for increased accuracy on a more powerful testing platform. This section represents some computational results of our proposed program.

A. Visual Results

a.) Results of SURF method

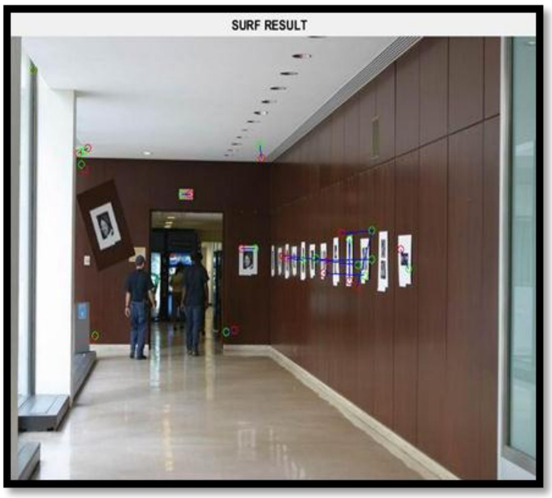


Fig.7. Forgery detected by SURF method

This screen shows that SURF extracts the features and descriptor vectors of the image. After extraction , matching of features that are extracted is done to locate the forged part in the digital image. Then Key-points are constructed and marked on the image which are shown with different colors.

b.) Results of SIFT method

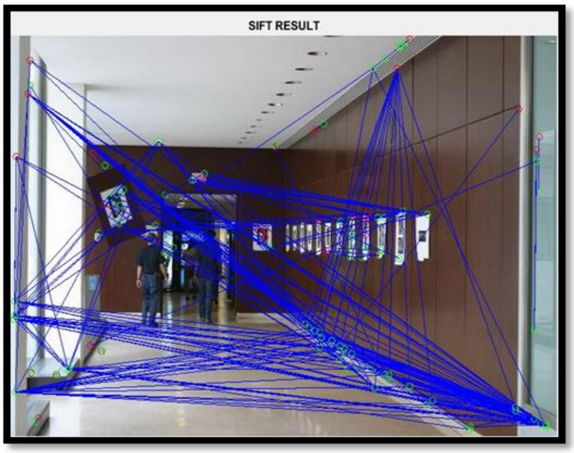


Fig.8. Forgery detected by SIFT method

This screen shows that Sift extracts features vectors and texture descriptors of an image. As most of the information is contained in actual part of image, so Sift is applied on it and it will give feature descriptors of interest key-points. After this matching is done to locate the forged regions.

c.) Results of combination of SIFT and SURF method

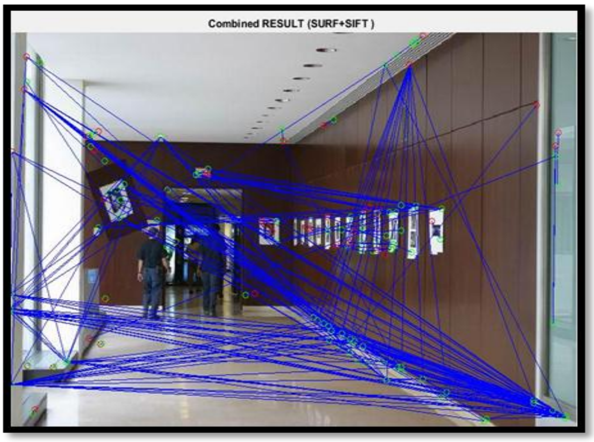


Fig.9. Forgery detected by combined work of SIFT and SURF method.

On this Screen, All the key-points that are marked by SIFT and SURF method uniquely are combined and then on the basis of theses key-points , matching is done to detect forgery.

d.) Accuracy Results Screen

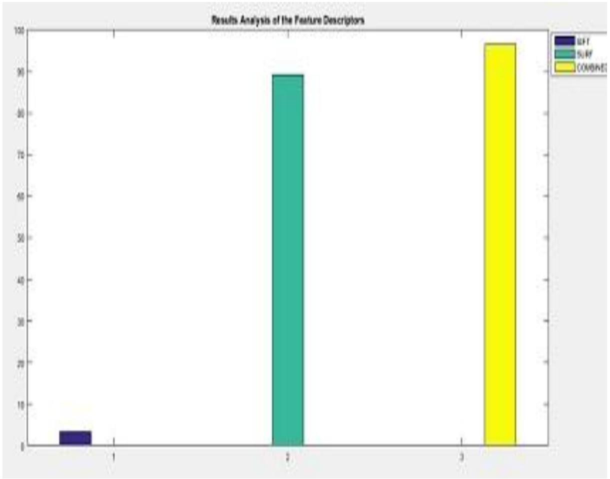


Fig.10. Accuracy comparison of proposed method with existing methods.

This screen shows the comparison of accuracy of proposed method with SIFT and SURF alone .From this figure it is clear that the accuracy is increased by combining two methods rather than apply SIFT and SURF alone. The combined accuracy is recorded as 96.40% but the accuracy of SURF alone is 89.1% and SIFT is 3 %.

B. Performance Display Evaluation Parameters

The following are important terminology, which are necessary to understand the performance measurements:

- **TP (True Positive):** is the number of tampered images, which are classified as tampered.
- **FN (False Negative):** is the number of tampered images, which are classified as authentic.
- **TN (True Negative):** is the number of authentic images, which are classified as authentic.
- **FP (False Positive):** is the number of authentic images, which are classified as tampered ones

For classification tasks, the terms true positives, true negatives, false positives, and false negatives compare the results of the classifier under test with trusted external judgments. The terms positive and negative refer to the classifier's prediction and the terms true and false refer to whether that prediction corresponds to the external judgment.

a.) Accuracy

Accuracy measures the percentage of the images that are correctly classified by the classifier. It is computed as :
Accuracy = (TP + TN) / (TP + TN + FN +FP)

Table 5.1 Shows overall accuracy of proposed model

TOTAL IMAGES TESTED	TRUE POSITIVE (TP)	TRUE NEGATIVE(TN)	FALSE POSITIVE(FP)	FALSE NEGATIVE(FN)	ACCURACY (IN %)
100	95	1	3	1	96.00%

In this table, 100 images are tested , out of which 95 images are successfully detected. The overall accuracy of proposed model is shown in the graph below:

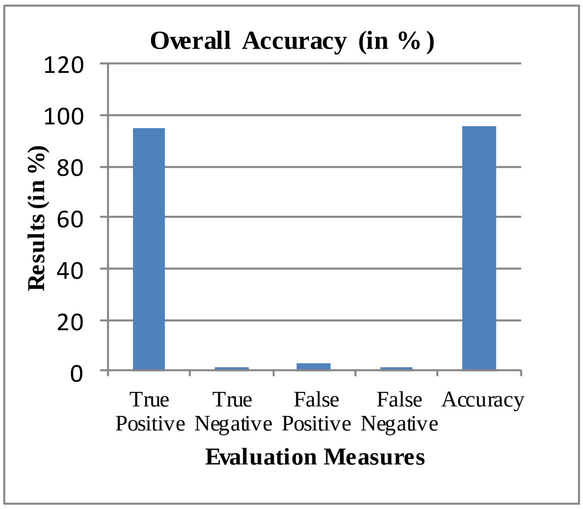


Fig.11. Shows overall accuracy of Proposed model.

This graph shows the true positive value i.e 95 which is successful detection of proposed model and total five failures occur , out of which one is True negative and False negative and three are False Positive and accuracy of proposed model is recorded as 96% as shown in the graph above.

b.) Precision

Precision is the fraction of retrieved instances that are relevant. It is based on measure of relevance. This is also known as Positive predictive value. It is calculated as:
Precision = TP / TP + FP

Table 5.2. Shows overall precision of proposed model

TOTAL IMAGES TESTED	TRUE POSITIVE(TP)	TRUE NEGATIVE(TN)	FALSE POSITIVE (FP)	FALSE NEGATIVE(FN)	PRECISION (IN %)
100	95	1	3	1	96.93%

In this table, 100 images are tested, out of which 95 images are detected successfully which is known as True positive. The overall precision is shown in the graph below:

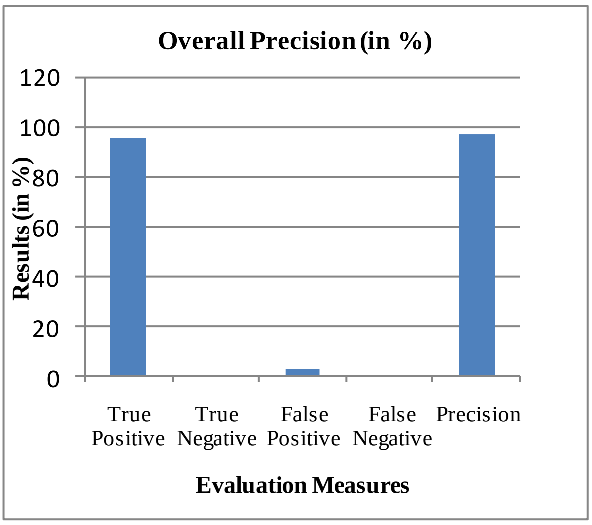


Fig.12. Shows overall Precision of Proposed model.

This graph shows the true positive value i.e 95 which is successful detection of proposed model and total five failures occur and accuracy of proposed model is recorded as 96% as shown in the graph above.

c.) Recall

Recall is defined as the fraction of relevant instances that are retrieved. It is based on an understanding and measure of relevance. This is also called sensitivity. It is calculated as:

Recall = TP / TP + FN

Table 5.3. Shows overall Recall value of proposed model

TOTAL IMAGES TESTED	TRUE POSITIVE(TP)	TRUE NEGATIVE(TN)	FALSE POSITIVE(FP)	FALSE NEGATIVE(FN)	RECALL(IN %)
100	95	1	3	1	98.00%

This table shows that total 100 images are tested and out of which 95 are successfully detected. On the basis of this recall is calculated and the graph for recall is shown below:

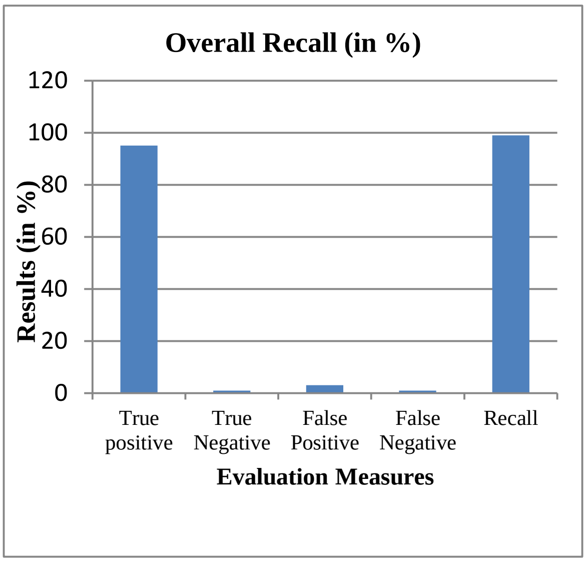


Fig.13. Shows overall Recall of Proposed model.

This graph shows the overall Recall of proposed model. The maximum precision that is recorded as 98 % which is shown in the graph above.

V. CONCLUSION AND FUTURE WORK

Since image forensics is a real world problem, a good forgery detection system should meet realistic requirements. In this paper various tampering detection tools can be applied to a wide variety of images. Two feature descriptor based algorithms namely SIFT and SURF are used together in a parallel manner. These algorithms are based on color and texture descriptor. The aim of these two algorithms is to extract features of digital image and then matching is done to check whether the image is forged or not. Parallel approach is used to increases the performance of the system. Feature detection algorithm works well for previously forged images. The proposed hybrid approach works well for both type of images: Bright color images and Low Brightness images. Also the accuracy of the results are increased by using these algorithms in parallel instead of using them separately. In future this work extended to improve the feature descriptor algorithm for enhance the speed and reduce the cost.

ACKNOWLEDGEMENT

This research paper is made possible through the help and support from everyone including teachers, parents, family and friends. Especially I would like to dedicate my acknowledgement of gratitude towards the following significant advisors and contributors. First and foremost, I would like to thank Mr. Manish Mahajan for his esteemed guidance and support. Finally, I sincerely thank my family for their patience and support. The product of this research paper would not be possible without all of them.

REFERENCES

[1] Christlein, V., Riess, C., Jordan, J., Riess, C., & Angelopoulou, E. (2012). An evaluation of popular copy-move forgery detection approaches.*Information Forensics and Security, IEEE Transactions on*, *7*(6), 1841-1854

[2] Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., & Serra, G. (2011). A sift-based forensic method for copy–move attack detection and transformation recovery. *Information Forensics and Security, IEEE Transactions on*, *6*(3), 1099-1110.

[3] Bo, X., Junwen, W., Guangjie, L., & Yuewei, D. (2010, November). Image copy-move forgery detection based on SURF. In *Multimedia Information Networking and Security (MINES), 2010 International Conference on* (pp. 889-892). IEEE.

[4] Hashmi, M. F., Hambarde, A. R., & Keskar, A. G. (2013, December). Copy move forgery detection using DWT and SIFT features. In *Intelligent Systems Design and Applications (ISDA), 2013 13th International Conference on* (pp. 188-193). IEEE

[5] Birajdar, G. K., & Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. *Digital Investigation*, *10*(3), 226-245.

[6] Sridevi, M., Mala, C., & Sanyam, S. (2012). Comparative study of image forgery and copy-move techniques. In *Advances in Computer Science, Engineering & Applications* (pp. 715-723). Springer Berlin Heidelberg.

[7] Sunil, K., Jagan, D., & Shaktidev, M. (2014). DCT-PCA based method for copy-move forgery detection. In *ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol II* (pp. 577-583). Springer International Publishing.

[8] S., & Das, P. K. (2011). Copy-move forgery detection in digital images: progress and challenges. *International Journal on Computer Science and Engineering*, *3*(2), 652-663.

[9] Jaberi, M., Bebis, G., Hussain, M., & Muhammad, G. (2014). Accurate and robust localization of duplicated region in copy–move image forgery.*Machine vision and applications*, *25*(2), 451-475.

[10] Muhammad, N., Hussain, M., Muhammad, G., & Bebis, G. (2011, August). Copy-move forgery detection using dyadic wavelet transform. In *Computer Graphics, Imaging and Visualization (CGIV), 2011 Eighth International Conference on* (pp. 103-108). IEEE.

[11] Cao, G., Zhao, Y., Ni, R., & Li, X. (2014). Contrast enhancement-based forensics in digital images. *Information Forensics and Security, IEEE Transactions on*, *9*(3), 515-525.

[12] Li, J., Li, X., Yang, B., & Sun, X. (2015). Segmentation-based image copy-move forgery detection scheme. *Information Forensics and Security, IEEE Transactions on*, *10*(3), 507-518.

[13] Ardizzone, E., Bruno, A., & Mazzola, G. (2010, September). Detecting multiple copies in tampered images. In *Image Processing (ICIP), 2010 17th IEEE International Conference on* (pp. 2117-2120). IEEE.

[14] Qian, R., Li, W., Yu, N., & Hao, Z. (2012, July). Image Forensics with Rotation-Tolerant Resampling Detection. In *Multimedia and Expo Workshops (ICMEW), 2012.*

[15] Li, J., Li, X., Yang, B., & Sun, X. (2015),"Segmentation-based image copy-move forgery detection scheme," Proc. IEEE *Transactions on Information Forensics and Security,* vol.*10*(3), pp.507-518.

[16] Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Del Tongo, L., & Serra, G. (2013), "Copy-move forgery detection and localization by means of robust clustering with J-Linkage," Proc. *Signal Processing: Image Communication*, vol.*28*(6), pp.659-669.

[17] Hsu, C. M., Lee, J. C., & Chen, W. K. (2015, May), " An Efficient Detection Algorithm for Copy-Move Forgery," Proc. *10th Asia Joint Conference on Information Security (AsiaJCIS)*, pp. 33-36.

[18] Wang, J., Yang, Z., & Niu, S. (2015), "Copy-Move Forgeries Detection Based on SIFT Algorithm," Proc. International Journal of Computer Science, pp.567-570.

[19] Panchal, P. M., Panchal, S. R., & Shah, S. K. (2013), "A comparison of SIFT and SURF," Proc. *International Journal of Innovative Research in Computer and Communication Engineering*, vol.*1*(2), 323-327.

[20] Cozzolino, D., Poggi, G., & Verdoliva, L. (2015), "Efficient Dense-Field Copy–Move Forgery Detection," Proc. IEEE *Transactions on Information Forensics and Security,* vol.10(11), pp.2284-2297.

[21] Ferrara, P., Bianchi, T., De Rosa, A., & Piva, A. (2013, September), "Reverse engineering of double compressed images in the presence of contrast enhancement," Proc. IEEE *15th International Workshop on Multimedia Signal Processing (MMSP*), pp. 141-146.

Authors' Profiles

Gurmeet Kaur, she is pursuing the master of technology from the CGC college of engineering (COE), Landran, PTU. She received her Bachelor of Technology in computer science from CTIEMT , Jalandar in 2014. Her area of interest is Digital Image Processing.

Manish Mahajan, He received his B.Tech in computer science from Kurukshetra University in 2004 and his M.Tech in 2006 from Punjab technical university (PTU). He is now a head of department, professor in CGC College of engineering, Landran, Mohali, India.. He has 11 years of teaching experience and 6 years of Research experience. His total publications are more than 50. His research interests include Image Processing and Information Security.

How to cite this paper: Gurmeet Kaur Saini, Manish Mahajan,"Improvement in Copy -Move Forgery Detection Using Hybrid Approach", International Journal of Modern Education and Computer Science(IJMECS), Vol.8, No.12, pp.56-63, 2016.DOI: 10.5815/ijmecs.2016.12.08