Proceedings of the 2nd International Conference on Communication and Electronics Systems (ICCES 2017)
IEEE Xplore Compliant - Part Number:CFP17AWO-ART, ISBN:978-1-5090-5013-0

Image forgery detection for high resolution images using SIFT and RANSAC algorithm

Gonapalli Ramu
M.Tech, Embedded Systems
Aditya Engineering College
Surampalem, Kakinada
Email: gonapalliramu@gmail.com

S.B.G. Thilak Babu
Assistant Professor
Aditya Engineering College
Surampalem, Kakinada
Email: thilaksayila@gmail.com

***Abstract*—Cloning (copy-move forgery) is a malicious tampering attack with digital images where a part of image is copied and pasted within the image to conceal the important details of image without any obvious traces of manipulation. This type of tampering attacks leaves a big question of authenticity of images to the forensics. Many techniques are proposed in the past few years after powerful software's are developed to manipulate the image. The proposed scheme is involved with both the block based and feature point extraction based techniques to extract the forged regions more accurately. The proposed algorithm mainly involves in matching the tentacles of same features extracted from each block by computing the dot product between the unit vectors. Random Sample Consensus (RANSAC) algorithm is used to extract the matched regions. The experimental result of the algorithm which is proposed indicates that, it can extract more accurate results compared with existing forgery detection methods.**

Keywords—DWT, SLIC, SIFT, Tentacles matching, RANSAC algorithm.

I. INTRODUCTION

Considering the popularity of digital images, image processing software technology also increased rapidly. This software's made the image manipulation easier. Majority considered passive tempering techniques are cloning, where a part or several regions of image is copied and they are pasted on the chosen regions. This type of tampering method is commonly used with scaling or compressing techniques on the copied part of image and in some conditions to make the forgery more efficient noise is also added with an intention to cover some evidences on the image. The existing techniques to detect the forged regions are block based and feature point based algorithms.

To overcome this copy and move forgery, many techniques are proposed. Image segmentation is one of the approaches where the image is segmented and overlapped. Principle component analysis (PCA) is used for deriving the alternative representation of the blocks. Later on, discrete wavelet transform (DWT) is used to extract the features directly from the image blocks and the overlapping blocks are reduced by using singular value decomposition (SVD). Further Fourier mellin transform (FMT) is used to apply on the image blocks where log polar values are represented as the block features.

(a) Original image (b) Forged image (c) Forged region detection

Fig.1. Example of copy move forged image

The above figure is example of the cloning technique where the region of image is copied and pasted within the image in such a way that it is not recognizable with naked eye. Considering this process as an illegal act, the appropriate technique should be developed.

- The proposed algorithm should detect every pixel element between objects.
- It should extract the exact and accurate forged regions with less complexity.

II. RELATED WORK

The important feature in the cloning to be considered is the copied and pasted parts of image are same. Hence we only discuss the passive algorithms to detect the forged area. Block-based and key-point-based algorithms are the two mostly used methods in the cloning detection technique. Fridrich et al. [2] describes about the block-based method using discrete cosine transform (DCT). The features are the quantized coefficients of (DCT) extracted from overlapping blocks. Popescu et al. [1] follows (PCA) for reduction of dimension for feature extraction. Further methods are involved with (DWT) and (SVD) algorithms to extract the feature points of image [3].

Key-point-based techniques also introduced to extract the forgery region. Scale invariant feature transform (SIFT) algorithm is used for extraction of key-points on the image [7], [4] and [9]. In [5] speed up Robust Features (SURF) is used to

find the forged part. In [10] local features are used to extract the interested points rather than using blocks for detection of tampering. These methods can identify the points matching but cannot locate the exact forged part in the image. Most of the block- based detection techniques uses the same algorithm but with different feature extraction techniques. These recall rates are considerable poor. Drawbacks are given as

- The over-lapping of rectangular blocks increase the complexity and expenses as the image size are increased.
- They are poor at defining the geometrical transformations of tampered image. As blocks are in rectangular shape it reduces the accuracy.
- Key-point based technique could overcome the above drawbacks but could not increase the recall rates.

III. PROPOSED ALGORITHM

To overcome the above drawbacks, we proposed a method where we use both block-based and the feature point-based algorithm. (DWT) is used for the image segmentation, where we use fourth level (DWT) to find the frequency energy coefficients. Considering the coefficients we calculate the initial size of the super pixel. This super pixel is used in SLIC algorithm to form the non-overlapping irregular blocks [11]. These non-overlapping irregular blocks give more accurate results for the high resolution images. To extract the features (SIFT) algorithm is applied to the irregular blocks. The feature are extracted in every irregular blocks, they are matched by calculating the Dot products between unit vectors. This gives the exact matched tentacles of (SIFT) feature in every block. Further (RANSAC) algorithm is applied to detect the forged regions.

A. Frequency distribution using DWT

As (DWT) is concentrated on both time and frequency, this transform gives good frequency and high temporal resolution for low and high frequency components. According to proposed algorithm (DWT) is applied using 'Haar' wavelet on to the image to verify whether the image is smooth or detailed image. This is done by calculating the low frequency energy. This process gives the appropriate frequency energy coefficients to calculate the initial size of the super pixel.

B. Extraction of super pixels

We gone through many experiments and found that better forgery regions are detected mostly in irregular blocks compared to regular blocks regions. However, (SLIC) cannot provide the initial size of the super pixel, the coefficients collected from (DWT) using 'Haar' wavelet is used to find the super pixel size S.

$$E^{LF} = \sum(|CA_4|) \tag{1}$$

$$E^{HF} = \sum_i(\sum|CD_i| + \sum|CH_i| + \sum|CV_i|), \quad i=1, 2.., 4 \tag{2}$$

ELF indicates low frequency energy; EHF indicates high frequency energy. CA gives the fourth approximation coefficients, whereas CD, CH, CV gives the detail coefficients.

Low frequency percentage is calculated as

$$P^{LF} = \frac{E^{LF}}{E^{LF}+E^{HF}} .100\% \tag{3}$$

$$S = \begin{cases} \sqrt{0.02XMXN}\,, P^{LF} > 50 \\ \sqrt{0.01XMXN}\,, P^{LF} \leq 50 \end{cases} \tag{4}$$

Using (4) we can calculate the size of S whereas MxN indicates the size of the input image. This calculation helps SLIC to give the meaningful non-overlapping irregular blocks.

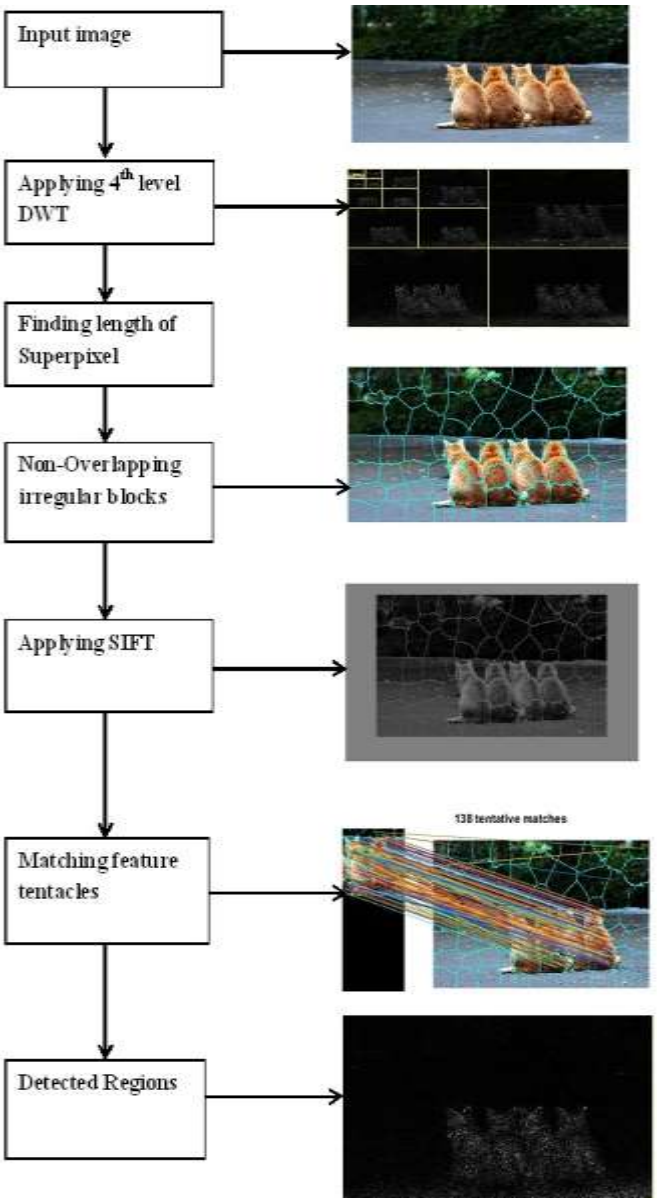


Fig.2. Proposed block diagram

C. Applyng SIFT transform

As SIFT and SURF are the transforms which are mostly used in feature extraction, but [9] shows that SIFT have more accuracy and can give better performance for the operation like scaling, blurring and compression. Considerable we use SIFT to extract the features points after applying SLIC algorithm. SIFT algorithm is designed with four main steps (1) scale space extrema detection, (2) key-point localization, (3) orientation assignment, (4) descriptor generation.

Initially using different values of sigma, in the Difference-of- Gaussian (DoG) function, it is required to identify the location and scaling points, this is done by Scale space extrema.

$$D(X,Y,\sigma) = (\big(G(x,y,k\sigma)G(x,y,\sigma)I(x,y)\big) \quad (5)$$

Here G is Gaussian function and I is given as the input image. Local minima and maxima of equation (5) are detected by comparing neighbour pixels of 3x3. Using key-point localization, we can reject the low contrast key-points. Orientation of key-points is done on basis of image gradient.

1) Sift discriptor generation: Gaussian blur level of the image to be selected using scale of keypoint. Image gradient magnitude is combined with the orientations and they are sampled according to the location of the key-point. This process allows for orientation invarience where the coordinate are rotated according to the keypoint orientation with some scale varience of 1.5 of gaussian function to generate key-point descriptors.

The key-point descriptors shown on the right are generated by orientation histogram over 4x4 sample regions.

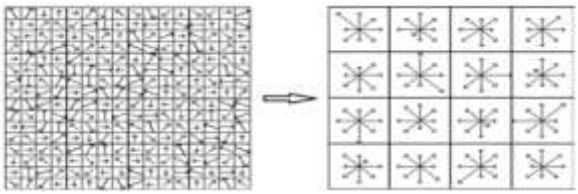


Fig.3. SIFT descriptor generation

In the above figure we can see that each histogram has 8 directions with length corresponding to the magnitude. It has 128 elements dimension of key-point descriptors where it uses 4x4 array location grid and 8 orientation bins in each sample

D. Feature matching

The extracted SIFT features in the irregular blocks are matched by computing the Dot products between unit vectors. This dot product calculates the sequence of two equal lengths and in return it gives a single number. It only matches the vector angles ratio which is less than the distance ratio of nearest and second nearest neighbor. The dot product is given as,

$$a.b = |ab^T| \quad (6)$$

Here b^T stands for the b transpose.

We have to check whether the nearest neighbor has angle less than distance ratio.

$$a.b = |a||b|\cos(\theta) \quad (7)$$

Now apply inverse cosine transform to the Dot product and match the nearest neighbor. RANSAC is the homographic strategy [8] which is mostly implemented. We use this algorithm to eliminate the unwanted matches. If at least 4 matches are found it will not be applied, this process gives the more reliable matches which are more compatible with homographic transformations.

- Chooses N information things at arbitrary.
- Evaluations parameter x.
- Discovers what number of information things (of M) fit the model with parameter vector x inside a client given resilience. Call this K.
- On the off chance that K is sufficiently huge, acknowledge fit and exit with progress.
- Rehash 1.4 L times.

We can discover L by the accompanying formulae:

$P_{fail} = Probability\ of\ L\ consecutive\ failures$

$P_{fail} = (Probability\ that\ given\ trail\ is\ a\ \ failures)L$

$P_{fail} = (1 - Probability\ of\ L\ consecutive\ success)L$

$P_{fail} = (1 - Probability\ that\ a\ random\ data\ item\ f\ its\ the\ model)N)L$

$P_{fail} = (1 - (P_g)^N)^L$

$L = \log(P_{fail}) \backslash \log(1 - (P_g)^N)$

IV. RESULTS

MATLAB is used to test the images where we had tested 80 images with resolutions between 1000 x 900 and 1200 x 1000.

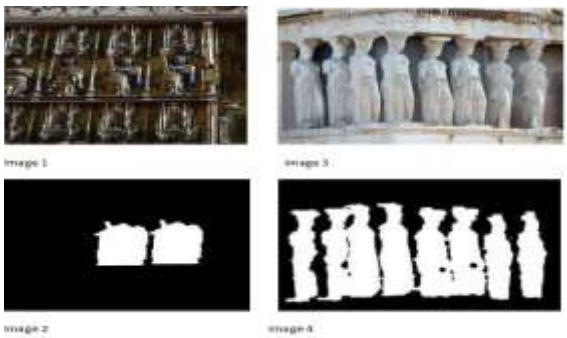


Fig.4. image1 and image 3 are host images and image 2 and image4 are detected regions

For the image1 shown in the above figure there are 379 feature points and tentacles matched were 142, for image3 there were 533 features and matched tentacles are 139. Here we define few terms for image accuracy, sensitivity, and specificity to verify the algorithm.

$$Sensitivity(S) = \frac{TP}{TP+FN} \quad (8)$$

$$Specificity(Sp) = \frac{TN}{TN+FP} \quad (9)$$

$$Accuracy(A) = \frac{TP+TN}{TN+TP+FN+FP} \quad (10)$$

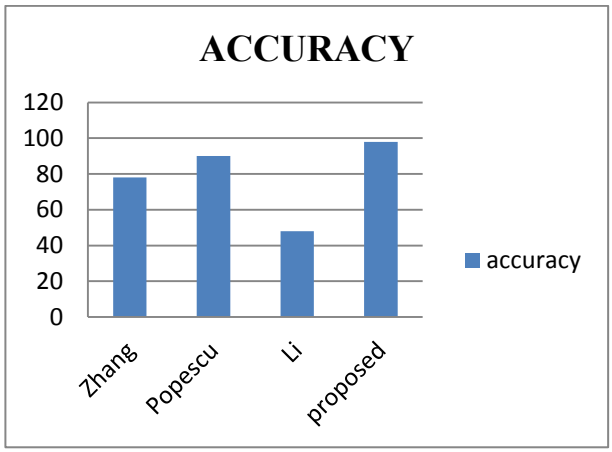
FPR= 1- specificity (FPR: False Positive Rate) (11)

FNR= 1- sensitivity (FNR: False Negative Rate) (12)

Here TP and TN is given as (true positive) and (true negative), when the identification of image is true i.e. forged or authentic. Here FP and FN which is given as (false positive) and (false negative), when the identification goes wrong and the result may i.e. forged or authentic [14].

TABLE I. PERFORMANCE CALCULATION OF PROPOSED ALGORITHM

Forged images	Unique images	Sensitivity	specificity	Accuracy	FPR	FNR
40	40	98%	96%	98%	8%	4%



The performance of the proposed scheme is defined by the calculation of precision and recall rates where precision is given as the ratio of forged pixels correctly detected and total forged pixels in the image. Recall rate is given as the ratio of forged pixels correctly detected and the forged pixels in the reference area of the image.

$$Precision = \frac{|\sigma \cap \sigma'|}{|\sigma|} \quad (13)$$

$$Recall = \frac{|\sigma \cap \sigma'|}{|\sigma'|} \quad (14)$$

TABLE II. DETECTION RESULTS AT PIXEL LEVEL

Methods	*Precision %*	*Recall %*
Wang [12]	*92.31*	*100*
Bravo [13]	*87.27*	*100*
SIFT [7][9]	*88.37*	*79.17*
SURF [5]	*91.49*	*89.52*
Proposed	*97*	*100*

Basically we performed with high resolution images giving more accuracy where comparitively above table provides some equal recall rates with block-based techniques [12, 13] but at high precision rates. This scheme giving more accurate results and performances proves to be a novel technique to be implemented

V. CONCLUSION

Many research papers have been reviewed; many forgery detection techniques are studied. The proposed method is robust as it uses SIFT algorithm, it is less complex and expensive as we adopted both block based and feature point based algorithms. We further used RANSAC algorithm to match the feature and extract the tampered region. The overall accuracy is 98 with data base of 80 images. The further work, we would like to implement the detection process with more recall rates and also with some other tampering techniques like splicing.

ACKNOWLEDGMENT

We would like to thank all the authors in the reference for providing great knowledge and helpful advices whenever required.

REFERENCES

[1] Popescu, A1in c., and Hany Farid, ”Exposing digital forgeries by detecting duplicated image regions”, Department of Computer Science, Dartmouth College, Technical Report. TR2004-515, August 2004.

[2] Fridrich, A. Jessica, B. David Soukal, and A. Jan Lukas, ”Detection of copy-move forgery in digital images”, In Proceedings of Digital Forensic Research Workshop. , Cleveland, OH, USA, pp. 55-61, August 2003.

[3] Li, Guohui, Qiong Wu, Dan Tu, and Shaojie Sun. ”A sorted neighbourhood approach for detecting duplicated regions in image forgeries based on DWT and SVD”, In Proceedings of IEEE International Conference on Multimedia and Expo., pp.1750-1753,2007.

[4] H. Huang, W. Guo, and Y. Zhang, Detection of copymove forgery in digital images using SIFT algorithm, in Proc. Pacific-Asia Workshop Comput. Intell. Ind. Appl. (PACIIA), Dec. 2008, pp. 272276.

[5] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, Image copymove forgery detection based on SURF, in Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES), Nov. 2010, pp. 889892.

[6] [6] R. Hartley and A. Zisserman. Multiple View Geometry in Computer Vision. Cambridge University Press, second edition, 2003).

[7] Amerini, Irene, et al. "A SIFT-based forensic method for copymove attack detection and transformation recovery." Information Forensics and Security, IEEE Transactions on 6.3 (2011): 1099-1110.

[8] J. J. Lee and G. Y. Kim. Robust estimation of camera homography using fuzzy RANSAC. In ICCSA '07: International Conference on Computational Science and Its Applications, 2007.

[9] D. G. Lowe, Object recognition from local scale-invariant features, in Proc. 7th IEEE Int. Conf. Comput. Vis., Sep. 1999, pp. 11501157.

[10] X. Pan and S. Lyu, Region duplication detection using image feature matching, IEEE Trans. Inf. Forensics Security, vol. 5, no. 4, pp. 857867, Dec. 2010.

[11] Chi-Man Pun, Xiao-Chen Yuan and Xiu-Li Bi, "Image forgery detection using Adaptive oversegmentation and feature point matching", IEEE Trans.Inf. Forensics Security, vol. 10, Aug 2015 .

[12] S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affectedby reflection, rotation and scaling," in *Proc. IEEE Int. Conf. Acoust.,*Speech, Signal Process. (ICASSP), May 2011, pp. 1880–1883.

[13] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, "Detection of image region duplication forgery using model with circle block," in *Proc. Int. Conf.* Multimedia Inf. Netw. Secur. (MINES), Nov. 2009, pp. 25–29.

[14] Mohmmad Farukh Hasmi, Aaditya R. Hambarde, Avinash G. Keskar, "copy move forgery dection using DWT and SIFT features", 2013, Int. Conf. Intelligent systems design and applications.