International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Image Forgery Detection with SIFT and RANSAC

Satish B Pratapur, Shubhangi D.C

Abstract— in this paper, simulations were performed using SIFT and RANSAC to highlight the forged regions in the doctored image. SIFT algorithm is modified to consider unit vectors as the features of the blocks. Blocks with similar unit vectors were grouped into cluster. Mean values of the clusters were compared to determine the similarity between clusters. Once the clusters were formed, the image was subjected to RANSAC algorithm to determine the geometric transformation and to highlight the forged region in the doctored image. Two simulations were performed to test the performance of the proposed method. First, doctored image with only scaling and next, image with both scaling and rotation were tested. The simulation results are presented in detail.

Index Terms—Image forgery detection, SIFT, RANSAC, Scaling, and Rotation.

I. INTRODUCTION

In today's world, there is more image data created than any other data type. For example, since majority of smart phones are equipped with high resolution cameras, users of the smart phones capture the important moments. Images convey large amount of information quickly. Images are also used as evidence in a court of law. Hence authenticity of these images when used as evidence must be considered before judging on the evidence. Also in other applications like military applications, important conclusions are drawn based on the pictures received by the establishments like intelligence bureaus. The actions planned based on image data would be very devastating if the image is not real. There can be a huge repercussions if the signature of the people is forged in property related documents, wills, cheques etc. In order to confuse the decision making process or cheat the authorities or people, images are manipulated by imposters to hide the truth. These kind of manipulated images convey false information. Digital forensic is a branch of science which deals with identifying the authenticity of the images to overcome these kind of problems and expose the falsehood.

Manuscript published on 30 September 2019
* Correspondence Author
Satish B Pratapur*, (Dept. of computer science & Engineering, VTU University, Belgavi-01
Dr.Shubhangi D.C, (Head of the Dept. of Computer Science & Engineering, VTU University, Belgavi-01.

Images may be copy pasted in certain regions. While there are many algorithms to detect a forged area of the image, Scale invariant feature transform or SIFT is an important algorithm since it is widely used for image feature extraction. Of many algorithm available today, Popescu et al. [1] proposed a method to determine the PCA components of different regions of the image.

The PCA components of different regions or blocks are determined using principle component analysis (PCA). While PCA is popularly used for dimensionality reductions, it can be used here to achieve a different objective. Fridrich et al. [2] proposed block based and key point technique to detect the forgery in the image. The block based and key point techniques are based on discrete cosine transform (DCT). Image is divided into many blocks and each block is subjected to DCT. These DCT coefficients are quantized and compared between the blocks. When the quantized coefficients of any two blocks are same, then the blocks are considered as duplicate or forged. There are other techniques like discrete wavelet transforms (DWT) which can be used in place of DCT to determine the similarity of different blocks in the image [3]. Also singular value decomposition can be used to derive the singular values of the blocks [3]. The singular values can be derived even if the block is in rectangular form. In PCA, it is possible to derive the coefficients only if the block is square in shape. This leads to higher computational time than those methods in which the rectangular shaped blocks can be treated.

DWT was also proposed by Mohammad et al. [4] for dimensionality reduction. It also improved the accuracy of solution. Forgery in the image was localized. A robust DCT based approach was proposed by Cao et al. [5] to determine the discrete coefficients.

A new method was proposed by Takwa et al. [6] using SIFT and SVD to automatically determine the copied regions to match the identical features. This method is capable to identifying even the carefully copied regions by professionals. It has used a hybrid method to combine the features of SIFT and SVD. In another SIFT based approach, the copy move forgery is detected with the help of Chan-Vese's Level Set. This approach was proposed by Sudhakar et al. [7]. Chan-Vese's Level Set approach was used to reduce the high volume of the features. It was possible to detect multiple forged regions and this method was invariant to scale and rotation. Highlights of this approach are ease of implementation and robustness. A SIFT based approach was also used to detect the forged areas in the image using geometric transformations [8] to check if there was any tampering. From the observation made in the current literature,

there is a need to improve the SIFT algorithm further to define the features in a more robust manner and it is attempted in this research work to propose an improved feature extraction method. In the next section, highlights of SIFT algorithm along with the proposed changes to SIFT is presented. In Sec. III, simulation results are presented for two cases, with scaling only and with scaling and rotation forgery. Finally important conclusions are drawn in Sec. IV.

II. SCALE-INVARIANT FEATURE TRANSFORM APPROACH

Image tampering methods can be divided into two classes, namely, active methods and passive methods. In active methods, some information is preserved in the image before the image is distributed for public consumption. The information can be embedded in the image during the creation of the image. One of the most popular methods to insert the information is through watermarking. Generally, image capturing devices like high end cameras, watermarking facility is available. Since watermarking of any image requires special hardware, it is not possible to insert water marking in the images that are captured by these cameras. However, such kind of doctored images are available in websites abundantly. If the images are watermarked with some information at the time of creation or distribution for public consumption, it is possible detect the image forgery with active methods.

In case of passive methods, no prior watermarking information is needed to determine if the image was actually forged. In this method, image is analyzed by studying the binary information of the image. The passive methods to detect the image forgery can be divided into two classes, namely, statistical methods and visual methods. In statistical methods, pixel intensities are used to detect the forgery and in case of visual method, forgery is detected by visual cues.

In visual method, the image is observed very carefully for the variation of the illumination effects on the image. The original image may have a very natural gradient on the image, but if it was forged, then there would be abrupt changes in the illumination. No special hardware is required to detect the image forgery in this case as human eye is enough to do the same. However, if the imposter is highly skilled in the domain of computer vision, there is a possibility to forge the image very professionally with the help of computer graphics. It may not be possible to differentiate the forged image from the original image at all. In such cases, forgery detection of the image with visual method fails.

In order to address the forgery problems created by professions, statistical methods can be used. Whenever some part of the image is to be hidden or if the meaning of the image needs to be changed, then some parts of the image are copied and pasted at other locations. Copy-move attack is performed in the same image. That means, some part of the image is copied and pasted at other location to hide the information. In case of splicing, some part of the image is copied and pasted in other images. In case of copy-move attack, the source and destination image are same. But this copy paste of a patch or tampered region on the image creates a clear demarcation at the boundary of the patch. In order to suppress the abrupt shift in the pixel values at the boundary of the patch, the boundary is blurred by the imposters.

Copy-Move Forgery challenges:

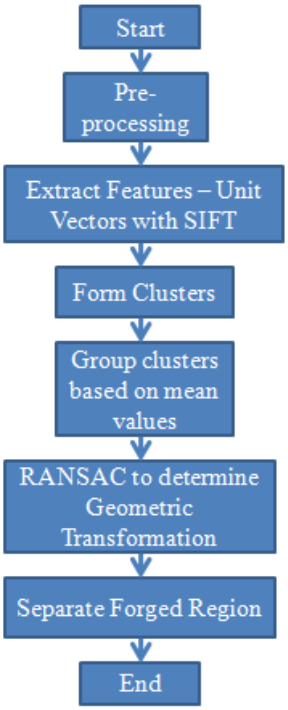
- The tampered region may not be same as original region.
- The forged image might have been preprocessed.
- Image might have been saved with lossy compression.
- Noise might have been added.
- Region might have been rotated before the forgery.
- Tampered region might have been blurred.
- Texture of tampered region might have been changed.
- Image might have been made lighter or darker.

In the present work, SIFT is implemented by extracting the global and local features first. The global features are block based features and local feature are key-point features. DWT is performed to derive the high frequency energy components of the blocks. All the blocks that have a very close match between the frequency components are grouped together. In this manner, super blocks are created and these super blocks are ensured to not overlapping with adjacent blocks [9]. Now, all the non over lapping large blocks are considered to be uniform within the blocks and non-uniform between the blocks.

The SIFT algorithm has several stages in which robust features are extracted to determine if an area of an image was indeed copy pasted. It is also possible to detect the geometrical transformations applied to forge the image. As a first step, noise in the image is required to be removed. The noise is that part of the image that has contaminated the image. It was not part of original image, but it was inserted to contaminate the image to hide some information or to change the meaning of the image. Noise can be removed by using Gaussian filters. One dimensional Gaussian filter can be applied to remove the noise. Later one more Gaussian filter pass can be applied on the output from the first Gaussian filter. . Other preprocessing steps involved are color space conversion and saliency map.

Feature extraction is the next step in which the image is subjected to feature extraction algorithm to extract distinct features from the image. Features are defined as interesting points or key points in the image which are based on color and texture values. In the proposed algorithm, unit vectors of the block are used as features.

Once the feature values are determined, they are formed into groups or clusters. All the features having similar values can be clustered using several techniques. Unsupervised learning techniques can be used to cluster the features or distance between the features can be calculated to group it into different clusters. A cluster will have center and it corresponds to the mean value of all the features in that cluster. Any feature is tested with it neighboring clusters to check if it falls into that cluster. All the clusters can be further grouped into smaller number of clusters. A SIFT may be run between these blocks to determine the dot product between the blocks. Flow charts of the forgery detection using SIFT and RANSAC:



III. SIMULATION RESULTS

In the simulations performed, an image is input to the model to determine the forged region in the image. Fig. 1 shows the original image for the purpose of reference and Fig. 2 shows the doctored image that was input to the SIFT model. Fig. 2 is processed by the SIFT model to determine the forged region in the image. It can be visually determined from the image that there is large region near the middle region of the image in which the shelf looks larger. This doctored image is input to the model to check if the model performs as expected. The model is expected to determine the forged regions in doctored image.

Figure 1: Original Image input to the model

Figure 2: Doctored Image input to the model

The doctored image is first subjected to noise removal. Noise removal can be performed in one stage itself or in multiple stages. In Fig. 3 first stage of noise removal is shown. First stage of Gaussian filter pass is applied to the image. It can be noticed that image gets blurred since some parts of the signal also gets removed along with noise. MATLAB was used to process the images at all stages. Similarly, second stage of noise removal was performed on the output of first stage Gaussian filter pass. Fig. 4 shows the image after the image subjected to second stage of Gaussian filter pass. Again the quality of image is reduced, but the aim of the noise reduction is to improve the signal to noise ratio.

Figure 3: Image after the first Gaussian Filter Pass

Figure 4: Image after the first Gaussian Filter Pass

The SIFT algorithm can be run on the doctored image to determine the unit vectors of all blocks. To do this, image was divided into many blocks and for each block features can be extracted.

In the present case, features are used to determine the orientation of each block. The orientation can be established with the help of unit vectors. It can be noticed from Fig. 5 that the unit vectors of some blocks that are found to be matching with other blocks are highlighted in red. The line direction can be considered as the direction of the block or orientation. Any two blocks have the same unit vectors are assumed to be a duplicate of the other blocks. Hence from the Fig. 5, it can be concluded that there are many blocks in the image that have the duplicates. These blocks can be grouped into clusters to form a large super block with the help of SIFT operators. The clusters can be grouped with the help of mean values of the cluster. The means of the clusters are compared and if they are very close to each other based on certain threshold value, then the two clusters can be grouped.

Figure 5: Image with Unit vectors estimated

Geometric transformations like scaling and rotation can be estimated by RANSAC algorithm. With the help of RANSAC and SIFT, it is possible to determine the amount of scaling performed on the forged area. Number of clusters matching with other clusters are identified and marked in the image. With this, the quantum of forgery can be estimated. Number of forged clusters in image shown in Fig. 1 are 98 with 15% of the clusters are doctored in image. The output of the SIFT-RANSAC algorithm that has output various parameters are:

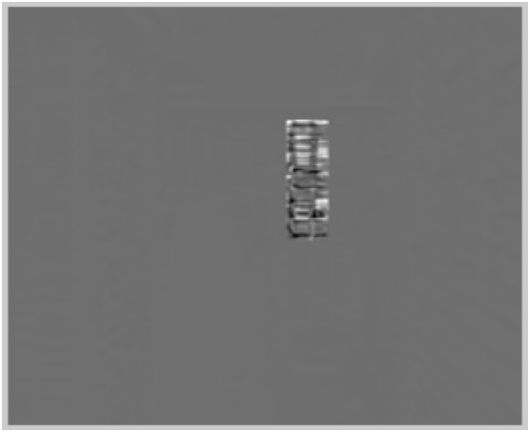


Figure 6: Separation of forged region

- Number of clusters detected as forgery is 98
- Forgery Detected area as percentage is 15%
- MSE (Mean Squared Error) = -0.026218
- SNR (Signal to Noise Ratio) = 69.999357
- PSNR (Signal to Noise Ratio) = 78.67
- AD (Average Difference) = -0.026218
- SC (Structural Content) = 1.024002
- NK (Normalised Cross-Correlation) = 0.985624
- MD (Maximum Difference) = 56.826089
- LMSE (Laplacian Mean Squared Error) = 0.287066
- NAE (Normalised Absolute Error) = 0.059290

Fig. 6 shows the separation of forged region from the doctored image for identification purpose. It does not remove the doctored region from the doctored image, but only highlights that portion for the user to understand the place of the forgery.

Figure 7: Original Image input to the model

In another experiment, another doctored image with not just scaling, but also a rotated forged region is input to the model. Fig. 7 shows the doctored image with forged region.

Again, purpose of this experiment is to check if the model can identify the region of forgery if scaling and rotation are involved.

Figure 8: Image after the first Gaussian Filter Pass

As processed in the first experiment, the doctored image is passed through two Gaussian filters to remove the noise. The signal to noise improved with the removal of noise. The more noise is removed, the better the identification of forged region possible. Hence noise removal plays an important role. Other preprocessing steps involved are color space conversion and saliency map. The preprocessing steps are necessary as mentioned before to improve the quality of image and hence to improve the ability to identify the forged region.

Figure 9: Image after the second Gaussian Filter Pass

When SIFT algorithm was run on the doctored image, the unit vectors of similar clusters are identified. The unit vectors are shown in Fig. 10. In this case also, image was divided into many blocks and features are extracted to determine the orientation of each block.

Figure 10: Image with Unit vectors estimated

All the blocks with almost similar unit vectors were grouped into clusters to form a large super block with the help of SIFT operators and mean values of the clusters. Means of the clusters were used to compare and to group the clusters.

Figure 11: Separation of forged region

Fig. 11 shows the separated region of the forgery from the doctored image. Again this is not a physical separation from the image, but only to highlight place of forgery on the image. In this image, the number of clusters detected as forgery is 137 and there is a forged area of 21%. The forged area was computed based on number of clusters identified as forgery and total number of clusters in the image. Various other parameters of the model are:

- Number of clusters detected as forgery is 137
- Forgery Detected area as percentage is 21%
- MSE (Mean Squared Error) = -0.023540
- SNR (Signal to Noise Ration) = 70.467260
- PSNR (Peak Signal to Noise Ration) = 81.5
- AD (Average Difference) = -0.023540
- SC (Structural Content) = 1.023595
- NK (Normalised Cross-Correlation) = 0.985914
- MD (Maximum Difference) = 54.865354
- LMSE (Laplacian Mean Squared Error) = 0.284880
- NAE (Normalised Absolute Error) = 0.058378

Table 1: Comparison of metrics with SIFT

Algorithm	PNSR	SNR	MSE	AD	SC	NK	MD	LMSE	NAE
DMD	76.2	56.6	1.3	45	78	1.67	88	2.5	0.67
Ref [11]	69.7	92.3	0.86	38	65	3.5	78	0.98	0.456
Ref [10]	82.3	67.8	1.15	26	89	2.4	87	0.89	0.44
DCT	90.1	96.8	1.43	17.9	56.8	0.99	21.7	0.34	0.019
CFA	84.7	72.6	0.72	60.98	68.7	0.369	92.3	2.3	0.62
ADQ	84.1	72.15	0.69	64.8	76.9	0.32	82.8	1.9	0.64
SIFT	81.5	70.46	0.023	0.023	1.023	0.98	54.86	0.28	0.058

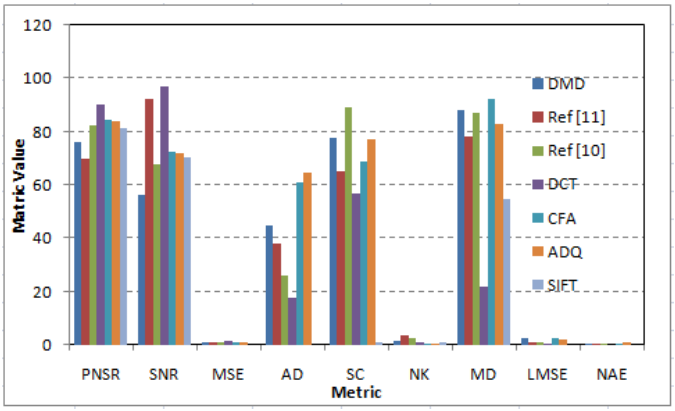


Figure 12: Comparison of metrics with SIFT

Table 1 and Fig. 12 shows the comparison of metrics like SNR, PNSR, Mean Squared Error (MSE), Average Difference (AD), Structural Content (SC), Normalized Cross-Correlation (NCC), Maximum Difference (MD), Laplacian MSE and Normalized Absolute Error (NAE) of SIFT with other six methods. It has been observed that SIFT outperformed over all other methods like Color Filter Array (CFA), Aligned Double Quantization (ADQ), Discrete Cosine Transform (DCT), DMD and other methods proposed in [10, 11] compared.

IV. CONCLUSIONS

In this paper, the SIFT algorithm is presented along with RANSAC to identify the forged region in the doctored images. The SIFT is modified to form the clusters based on unit vectors instead of pixel intensities. Initially, image is divided into blocks and unit vectors of each block are determined. The unit vectors of similar blocks are compared and formed into clusters based on the mean values. A super block is formed by merging all the blocks of similar unit vectors. A RANSAC algorithm is run on the super blocks to determine the geometric transformation and highlight the forged regions. When two experiments were conducted to test the performance of the model, it is found that there was 15% and 21% of area of the images was forged respectively in two different images. In the first image, only scaling was performed in forgery where as in second case, both scaling and rotation was performed. Various parameters of the model were derived. Overall, the algorithm has produced very good accuracy of identification of forged regions in the doctored images.

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, ”D etection 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
4. Multimedia and Expo., pp.1750-1753,2007.
5. Mohammad Farukh Hashmi, Aaditya R. Hambarde, Avinash G. Keskar, , 2013, “Copy Move Forgery Detection using DWT and SIFT Features”, IEEE 13thInternation Conference on Intelligent Systems Design and applications.
6. Yanjun Cao, T. Gao, and qunting Yang, 2012, “A Robust Detecton algorithm for Copy-Move Forgery in Digital Images”, Forensic Int. Volume 214, pp. 33-43.
7. Takwa Chihaoui, Sami Bourouis, and Kamel hamrouni, 2014, “Copy-Move Image Forgery Detection based on SIFT Descriptors and SVD-Matching”, 1st International Conference on Advanced Technologies for Signal and Image Processing-ATSIP’2014, Sousse, Tunisia.
8. Sudhakar. K, Sandeep V.M, Subhash Kulkarni, 2014, “Speeding-Up SIFT based Copy-Move Forgery Detection Using Level set Approach”, International Conference on Advances in Electronics, Computers and Communications (ICAECC).
9. L.Kang, X.-P. Cheng, 2010, “Copy-Move Forgery Detection in Digital Image”, 3rd International Congress on Image and Signal Processing, IEEE Computer Society, pp. 2419-21.
10. Gonapalli Ramu and S.B.G. Thilak Babu, Image forgery detection for high resolution images using SIFT and RANSAC algorithm, 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.
11. T. Bianchi,et.al, "Analysis of Non-Aligned Double JPEG Artifacts for the Localization of Image Forgeries" , WIFS‘2011, November 29th-December 2nd, 2011, Foz do Iguac¸u, Brazil. 978-1-4577-1019-3/11/ 2011 IEEE.
12. T.-T. Ng et.al, “Physics-motivated features for distinguishing photographic images and computer graphics” in ACM Intl. Conference on Multimedia, ser. MULTIMEDIA'05, 2005, pp. 239–248.

AUTHORS PROFILE

Asst.Prof.SATISH B PRATAPUR pursed Bachelor of Engineering in Computer Science and Engineering from Visvesvaraya Technological University, Belgavi, India in 2009 and Master of Technology from Visvesvaraya Technological University, Belgavi, India in the year 2011. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Sciences & Engineering in Appa Institute of Engg. & Technology, Kalaburgi, India since 2011. He has published a two papers in international journals. His main research work focuses on Image processing, Cryptography Algorithms. He has 8 years of teaching experience.

Dr.SHUBHANGI D CHITKE pursed Bachelor of Engineering in Electronics & Communication Engineering in 1995 from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad and Master of Technology in Computer Science and Engineering from Visvesvaraya Technological University, Belgavi, India in year 2000. Completed PhD in 2010 from Computer Science and Engineering in MGR University, Chennai. She has published more than 87 research papers in international journals and 9 international conference papers. She had received two best paper awards. Her area of research is Machine Learning, Image Processing, Cloud Computing Security, Big Data Analytics, IOT and Pattern Recognition. She has 21 years of teaching experience and 8 years of Research Experience. She is presently working as a Professor in Department of PG Studies in Computer Science and Engineering from Visvesvaraya Technological University, Kalaburgi, India.