Volume 6, Issue 1, January 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Detecting the Image Forgery from Color Images Using SURF and DWT

Jasdeep Kaur Dhillon, Jyoti Rani
Department of Computer &Science Engineering,
GZS PTU Campus, Bathinda, Punjab, India

Abstract—Forensics means the use of science and technology in the investigation and establishment of facts. So the photos or different pictures can be transmitted to and reconverted into pictures by another PC. Computerized crime scene investigation (in some cases known as advanced legal science) is a branch of measurable science including the recuperation and examination of material found in computerized gadgets. Advanced picture crime scene investigation goes for recovering so as to approve the genuineness of pictures data about their history. Two primary issues are tended to: the recognizable proof of the imaging gadget that caught the picture, and the identification of hints of phonies. These days, because of the promising results achieved by ahead of schedule studies and to the continually developing number of uses, advanced picture legal sciences speak to an engaging examination area for some scientists. With the across the board accessibility of picture altering programming, advanced pictures have been turning out to be anything but difficult to control and alter notwithstanding for non-proficient clients. Picture control has gotten to be typical with developing simple access to effective registering capacities. A standout amongst the most widely recognized sorts of picture imitations is the duplicate glue falsification, wherein a district from a picture is supplanted with another area from the same picture (With conceivable changes). Since the replicated part originate from the same picture, its critical properties, for example, clamor, shading palette and Composition will be perfect with whatever is left of the picture and hence will be harder to recognize and identify these parts. Computerized picture crime scene investigation is a fresh out of the plastic new research field which goes for recovering so as to approve the legitimacy of pictures data about their history. Computerized picture criminology goes for recovering so as to approve the validness of pictures data about their history. We propose a progression of calculations which are mix of speeded-up strong component changes and Wavelet Transforms. In doing as such we will first examine Speeded-Up Robust Feature (SURF), SURF in mix with Discrete Wavelet Transform (DWT), SURF in mix with Discrete Wavelet Transform (DWT). These calculations are not the same as the beforehand proposed calculation in the way that they are connected on the whole picture to concentrate highlights instead of separating the picture into the squares. From the outcomes got we have the capacity to close the proposed calculations are superior to their partners both as far as computational multifaceted nature and invariance to scale and pivot furthermore for the blend of assaults. We have located the 97% precision of the work.

Keywords— Digital Image forgery, DWT (Discrete Wavelet Transform), SURF (Speeded-Up Robust Feature), Image, Forensics etc.

I. INTRODUCTION

Digital image forensics aims at validating the authenticity of images by recovering information about their history. Copy-paste forgery, wherein a region from an image is replaced with another region from the same image (with possible transformations). Because the copied part come from the same image, its important properties, such as noise, color palette and texture, will be compatible with the rest of the image and thus will be more difficult to distinguish and detect these parts. Digital image forensics is a brand new research field which aims at validating the authenticity of images by recovering information about their history. The fundamental problems which research found in the literature can be categorized into the natural, forgery detection, flow mapping, and source identification. Therefore, the originality and authenticity of images or data in many cases become challenging problem. Researchers have related the natural issues to the advance in computer graphics, animation, multimedia in the association of high computing machines, algorithms, increases the complexity of the issue.

II. PROPOSED METHODOLOGY

In this paper, we have implemented a technique for copy paste forgery detection. Firstly the DWT technique is applied on the particular image and then SURF is applied .In the next part the hybrid of these two techniques i.e.DWT+SURF is applied which helps to obtain the copy paste part of an image.

A. DWT

The discrete wavelet change (DWT) is an execution of the wavelet change utilizing a discrete arrangement of the wavelet scales and interpretations complying with some characterized guidelines. The idea for using this is due to its inherent

multiresolution characteristics. The basic idea is to reduce the size of the image at each level 2^j*2^j pixel at level L reduces to $2^{j/2}*2^{j/2}$ at level L+1.Further decomposition to vertical, horizontal and diagonal components of the image. DWT is applied on the given image to disintegrate the image into four sub-images i.e. LL, LH, HL, HH.

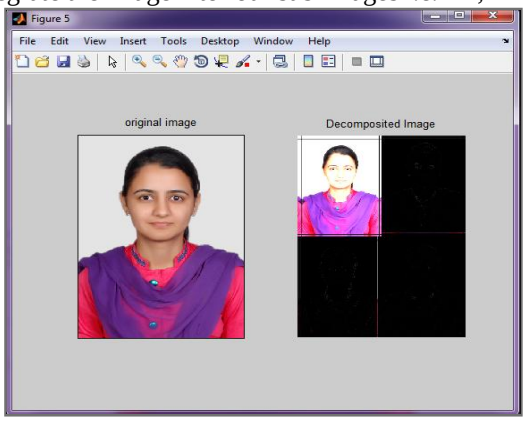

Figure 1: Shows the DWT is applied and decomposition is done on LL part

The complete flow of the algorithm is presented in the Fig.

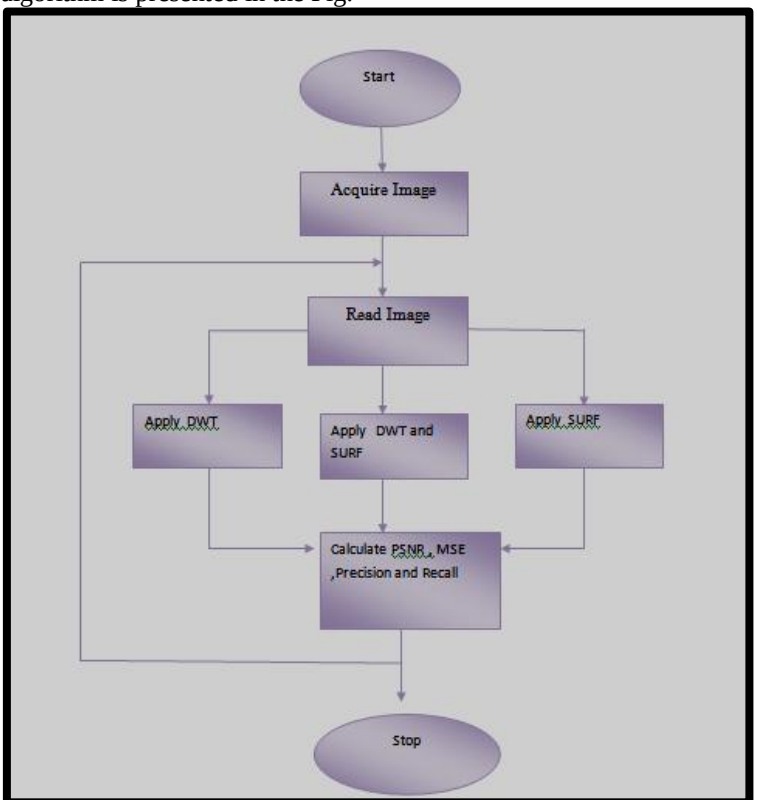

Figure 2: shows the methodology that is followed

B. SURF

SURF (Speeded-Up Robust Feature) was first presented by Bay et al. [19] and is used to obtain scale and rotation invariant detector as well as descriptor. SURF is better than other methods in terms of repeatability, distinctiveness, and faster computational time. SURF generally consists of detection of interest point and interest point descriptor generation.

C. DWT+SURF

In this part we are going to propose a new algorithm which combines both the techniques DWT with SURF. Here first DWT is applied on the given image and we apply SURF on the LL part to obtain key points and there corresponding descriptors.

III. TEST OF ROBUSTNESS AGAINST VARIOUS ATTACKS

A. DWT +SURF

With the help of this paper we present a new method of diagnosing copy move image forgery using SURF with DWT. As shown in the flow chart above first DWT is applied on the image and then we apply SURF on the LL part of the image. Since SURF will provide us with key points and there corresponding descriptor vectors among which we have to find similarity in order to infer whether the forgery has been done or not.

Figure 3: shows the image that is browsed for the process

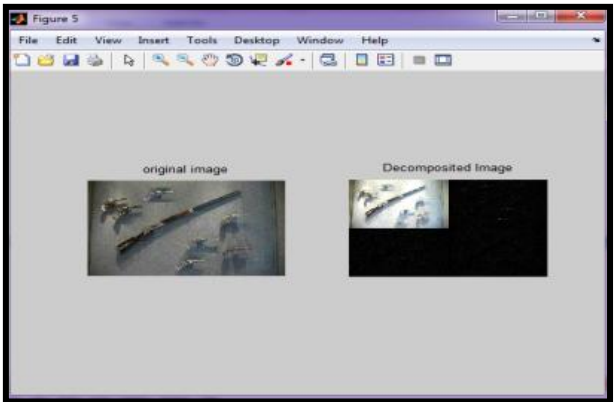

Figure 4: shows the image that is decomposed in DWT

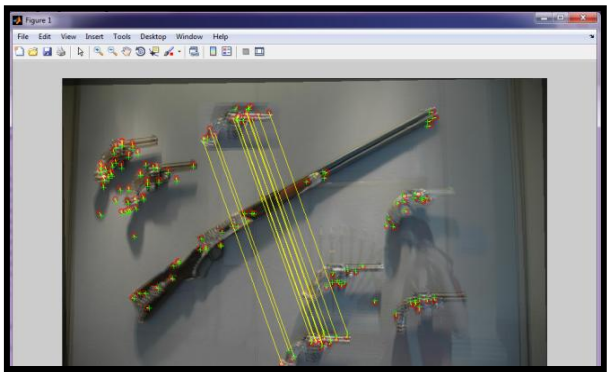

Figure 5: shows the copy paste part is detected from the image

IV. SIMULATION RESULTS AND EVALUTION OF PERFORMANCE PARAMETERS

In result analysis, we applied the proposed algorithm over a standard dataset MICC-F220 [8]. This simulation has been performed on MATLAB 2012a software with 32GB Ram and core i7 processor.

We are focusing on two major performance parameters at the image level to determine the fact that an image has been tampered or not. Considering the image level some of the important measures are described in Table I.

Table I. Evalution Measures Description

Evaluation Measures	**Description**
True Positive (TP)	Number of images that have been correctly detected as forged
False Positive (Fp)	Number of images that have been falsely detected as forged
False Negative (FN)	Number of images that have been falsely missed but they are forged.
True Negative (TN)	Number of images that have been correctly detected as not-forged

From the above mentioned measures we calculated Precision, *p,* and *Recall, r* which are defined as:

$$p = \frac{Tp}{Tp+Fp} \text{ and } r = \frac{Tp}{Tp+Fn}$$

Precision represents the probability that detected forgery is truly a forgery and *Recall* represents probability that a forged image has been detected. *Recall* is also called as True Positive Rate (TPR) [22].

Table II. Parameters Evaluated With Hybrid Technique

Parameters	**Description**
Precision	97.0689%
Recall	15.67161%
PSNR	38.3772%
MSE	17.48663%

Table III. Comparison With Previous Algorithms

Name of Image	**Precision**
Our Result	97.0689%
Mishra et al.	73.64%
M.F.Hashmi	64%

V. CONCLUSION

In response to forgery growth, researchers have begun developing digital forensic techniques capable of identifying digital replication. These forensic techniques operate by detecting imperceptible traces left by editing operations in digital multimedia content. In this dissertation, we propose several new digital forensic techniques to detect evidence of editing in digital multimedia content. We are using DWT, SURF and DWT+SURF for forensic tasks such as identifying cut-and-paste forgeries from JPEG compressed images. In this the Precision, recall, PSNR and MSE is calculated to analyse the detected part of the forged image. The Overall result is calculated in this work is 97.0689%.

REFERENCES

[1] Mohammad Farukh Hashmi "Passive detection of copy move forgery using Wavelet transform and SIFT features"in Journal of Information Assurance and Security,ISSN 1554-1010,volume 9,Page no 197-204,(2014)

[2] Salma Amtullah, Dr. Ajay Koul "Passive Image Forensic Method to detect Copy Move Forgery in Digital Images" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XII, Page no 96-104. (Mar-Apr. 2014).

[3] Tushant A. Kohale*, Prof. P. R. Lakhe " Detection of Post operated Copy Move Image Forgery by Integrating Block Based and Feature Based Method" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, ISSN: 2277 128X (January 2014).

[4] Mohammad Farukh Hashmi "Passive detection of copy move forgery using Wavelet transform and SIFT features"in Journal of Information Assurance and Security,ISSN 1554-1010,volume 9,Page no 197-204,(2014).

[5] Chen, L., Lu, W., Ni, J., Sun, W., & Huang, J. Region duplication detection based on Harris corner points and step sector statistics. Journal of Visual Communication and Image Representation, 24(3), Page no 244-254 (2013).

[6] M.Sridevi "copy – move image forgery detection in a parallel environment," SIPM, FCST, ITCA, WSE, ACSIT, CS & IT 06, Page no. 19–29,(2012).

[7] Mohamadian Zahra, "Image Duplication Forgery Detection using Two Robust Features," in ISSN 2277-2502 Volume 1(12), 1-6, December (2012).

[8] Yadav, P., Rathore, Y., &Yadu, A. DWT Based Copy-Move Image Forgery Detection. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), 1(5), 56-58 (2012).

[9] Pan, X. Z., & Wang, H. M. The Detection Method of Image Regional Forgery Based DWT and 2DIMPCA.Advanced Materials Research, 532, 692-696 (2012).

[10] Pujari, V. S.,& Sohani, M. A Comparative Analysis on Copy Move Forgery Detection Using Frequency Domain Techniques. International Journal of Global Technology Initiatives, 1(1), E104-E111 (2012).

[11] Pan, X. Z., & Wang, H. M. The Detection Method of Image Regional Forgery Based DWT and 2DIMPCA.Advanced Materials Research, 532, 692-696 (2012).

[12] Amerini "A SIFT-based forensic method for copy-move attack detection and transformation recovery "published in IEEE TIFS, volume 6, September (2011).

[13] Liu, M.-H., & Xu, W.-H. Detection of copy-move forgery image based on fractal and statistics. Journal of Computer Applications, 8, 061 (2011).

[14] Yao, H., Qiao, T., Tang, Z., Zhao, Y., & Mao, H. Detecting Copy-Move Forgery Using Non-negative Matrix Factorization. Paper presented at the Third International Conference on Multimedia Information Networking and Security (MINES) (2011).

[15] P.Kakar and N.Sudha "Exposing Post processed Copy-Paste Forgeries through Transform-Invariant Features", volume 206, no. 1-3, Page no. 178–184, (2011).

[16] A.N.Myna "Signal Processing: Image Communication" 25 Page no 389–399(2010)

[17] M.C.Stamnn,"Forensics Detection of Image Manipulation Using Statistical Intrinsic Fingerprints", IEEE Transactions on information Forensics and Security, volume 5 No 3, (2010).

[18] Saiqa Khan An Efficient Method for Detection of Copy-Move Forgery Using Discrete Wavelet International Journal on Computer Science and Engineering Volume 02, No. 05, 1801-1806 (2010).

[19] S.Khan and A.Kulkarni, "Reduced Time Complexity for Detection of Copy-Move Forgery Using Discrete Wavelet Transform" International Journal of Computer Applications (0975 – 8887) Volume 6– No.7, September (2010).

[20] Li Kang "Image and Signal Processing" (CISP), 2010 3rd International Congress on Volume:5 , Page no 2419 – 2421,(2010)

[21] S.Bayram, H.T.Sencar and N.Menon"A Survey of Copy-Move Forgery Detection Techniques", submitted to ICASSP (2009).

[22] M. Chen, J. Fridrich, M. Goljan, and J. Lukáˇs, "Determining image origin and integrity using sensor noise," IEEE Trans. Inf. Forensics Security, volume 3, no. 1, Page no. 74–90, March (2008).

[23] M. K. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments," IEEE Trans. Inf. Forensics Security, volume 2, no.3, Page no 450–461, September (2007).

[24] S. Bayram, I.Avcibas, B. Sankur, and N. Memon, "Image manipulation detection," J. Electron. Image, volume 15, no. 4, Page no 041102, (2006).

[25] A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," IEEE Transactions on Signal Processing, volume 53(2), Page no. 758–767, (2005).

[26] Dhara Anandpara" A Joint Forensic System to Detect Image Forgery using Copy Move Forgery Detection and Double JPEG Compression Approaches" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.

[27] M.K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," Proc. ACM Multimedia and Security Workshop, New York, Page no.1–9, (2005).

[28] T.-T. Ng, S.-F. Chang, J. Hsu, L. Xie, and M. P. Tsui, "Physics-motivated features for distinguishing photographic images and computer graphics," in Proc. ACM Multimedia, Singapore, Page no. 239–248 (2005).

