Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 06, June-2016

Detection of Digital Image Forgery using Transformation Domain

Dhanshree P. Patil
Computer Science Department
Astral Institute of Technology & Research
Indore, India

Lakshita Landge
Computer Science Department
Astral Institute of Technology & Research
Indore, India

***Abstract*— Digital transformation has witnessed a momentous growth over the last decade, which also reflects in widespread use of digital images in daily life. Today digital images are widely used in critical areas such as judiciary, commerce, politics, surveillance and journalism. This widespread growth in digital images has also seen equivalent growth in inexpensive, easy to access and sophisticated image editing tools. These tools have flourished the growth in image manipulation. While there are multiple techniques of digital image forgery detection, we have dedicated our research effort towards pixel based forensic techniques. These techniques use block based detection algorithm using transform domain. This paper showcases that the detection accuracy of our proposed algorithm based on Stationary Wavelet Transform (SWT) is higher than the one based on Discrete Wavelet Transform (DWT) due to better decomposition of image using multiple filtering levels.**

Keywords*— *Copy-move forgery, splicing, block based, transform domain, SWT, DWT

I. INTRODUCTION

Authenticity of digital images is of paramount importance. This in today’s time is more admissible than any before due to criticality they have assumed in recent times across widespread applications. Simultaneously there is equivalent growth in inexpensive, easy to access and sophisticated image manipulating tools for e.g. Adobe Photoshop, GIMP, and Inscape to name a few. This has generated lot of interest for people wanting to manipulate the digital images with easily accessible and inexpensive and variety of common editing tools.

These factors lead to increasing cases of image forgery, posing challenges to the very use of digital images in the critical application areas. The most common ones include judiciary, surveillance, crime, sports, journalism, medical diagnostics and assessment of claim settlements for the insured properties.

In this paper, we have analysed the landscape of different types of digital image forgery techniques and the motivations behind them. Among these types, we focus on detecting the most common type of digital forgery – the copy-move attack and splicing. Our objective is to focus on highlighting areas within the image that are masked or tampered with. We plan to overcome the challenges faced by existing forgery detection algorithms in identifying the correct forged region and also to improve the detection accuracy based on transforms.

II. OVERVIEW OF DIGITAL IMAGE FORENSICS

A. Types of forgeries

Digital image forgeries can be classified into three broad categories [1, 2]. Copy move forgery is the most popular and hard to detect picture tampering method. Within this manipulation method a part of the identical picture is copied and pasted into another part of that image itself. In a copy-move attack, the purpose is to cover something in the authentic photo with a few other part of the same photo.

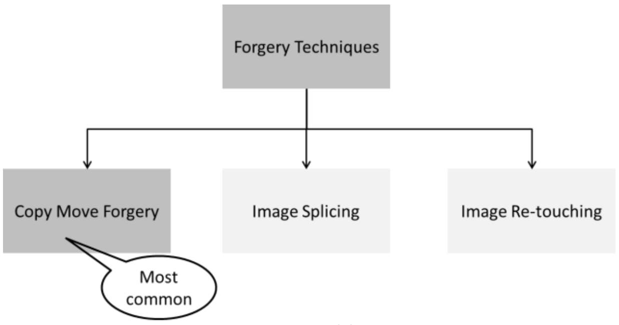

Fig 1. Types of forgeries

B. Types of forensic techniques

Digital forensic techniques are broadly classified as Active and Passive. Active techniques require known validation code embedded into the core image content before distributing image into a potentially unsecure domain with likelihood of tampering incidences. During the authentication process of the image, the presence of validation code is tested in the image content. Digital watermarking and digital signatures are one of the most popular active forgery detection techniques. However these techniques require hardware or software to pre-embed the validation code prior to the distribution. Passive techniques of image forgery detection however do not require any pre-requisites. These techniques rely on the principle that the image processing activities render unique traces (i.e. intrinsic fingerprints) on the altered images. This paper explores various image forensic techniques that uncover variety of forgeries.

Our proposed approach is based on pixel based technique. The pixel-based photo forgery detection aims to verify the authenticity of virtual photographs when there is no history statistics available and nature of forgery. In this paper we have discussed various pixel-based techniques for image forgery detection, mainly copy-move and splicing techniques.

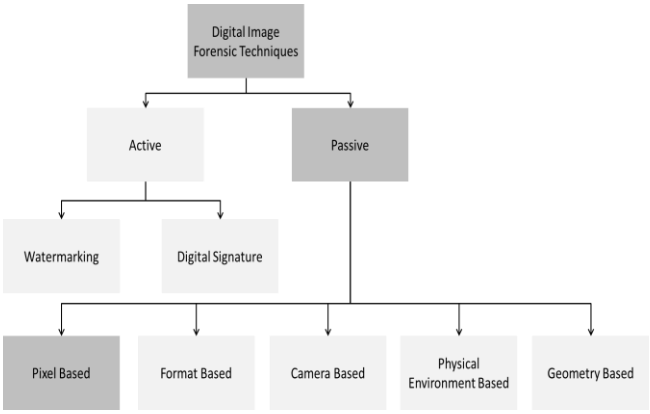

Fig 2. Image authentication techniques

III. LITERATURE SURVEY

Popescu and Farid [3] proposed a method in 2004 for identifying forged regions within image. The technique was based on PCA, where authors used a relatively smaller fix sized blocks within the image (16*16 or 32*32) and applied PCA on them. The algorithm involved calculation of the eigenvectors and eigenvalues for each such block. Post that the blocks were sorted lexicographically; in order to identify duplicate regions. This algorithm was more efficient and robust compared to earlier work of detecting a forged image automatically.

Xiao Bing and Sheng Min [4] proposed the forgery detection technique based on SVD to identify forged regions in copy move forgery in 2008. The authors used SVD to extract feature vector both algebraic and geometric invariant, and further reduced the dimension representation. Similar bocks of image were identified using lexicographical sorting to rows and column vectors to detect forged regions. This algorithm turned out to be more efficient as the computational complexity was reduced. Also it provided robust results against retouching operations.

Huang et al. [5], proposed an improvement over the work done by Fridrich et al., in terms of processing speed in 2011. The algorithm is based on DCT to find feature vectors followed by usage of matching operations to detect forged regions. This algorithm is relatively simpler, and detects duplicate areas within the image with higher accuracy.

Muhammad et al. [6], developed a technique using dyadic wavelet transform (DyWT) for detection of copy-move forgery in 2012. The authors have divided image into approximate and definite sub-bands, which were subsequently fragmented into overlapping blocks. The parameter extraction of blocks was performed for the comparison and similarity calculation. Blocks were paired based on the similarity in the features and then a user defined threshold was used to detect pairs that do not match with the majority blocks of the image. The output of the algorithm highlights forged regions within the image. This algorithm falls short in terms of manual definition of threshold to identify forged regions in the image.

Xufeng Lin, Chang-Tsun Li and Yongjian Hu [7] proposed a novel method of digital image forensic using inter-channel similarities in high value frequency components of images to detect contrast enhancement and expose copy move image forgery. This technique overcame the limitations of earlier technique from Stamm and Liu where user had to define optimal parameters of pinch off function and cut off frequency.

IV. PROPOSED METHODOLOGY

A. *Block based forensic methodologies*

Passive strategies of virtual image forensic have wider coverage throughout distinctive methodologies. The reproduction flow forgery detection techniques based on pixels are broadly categorised into two kinds of methods: ‘block based’ and ‘brute force’.

Block based matching techniques score better compared to brute force methodology. As exact matching of blocks is not effective in many cases where post processing operations on the forged areas destroy their original values. In this paper, we have used transform domain based methodology to extract features of the blocks and perform inter block comparison to ascertain the potential suspect regions in the input image.

B. *Transform domain*

Our proposed methodology highlights the base utility of DWT in block matching while forger detection, and compares its results against an enhanced transform which is time invariant – Stationary Wavelet Transform (SWT).

Discrete wavelet transform possess a critical shortcoming. It is a time variant transformation function, which means it does not reflect any translation of input signal into the transformed version. In order to overcome this limitation, Stationary wavelet transform was proposed where decimators were omitted in wavelet decomposition and in every decomposition level the identical period of coefficients have been kept. At the price of greater computation and storage, we can get the SWT that is shift invariance.

SWT is used within the proposed technique to enhance the approximation of the picture capabilities through multiple levels of definite coefficients obtained through up-sampling and down-sampling of approximate coefficients from previous level of signal exploration.

C. *Proposed Methodology*

In this paper, we have adopted the block matching methodology of pixel based techniques. We have proposed use of SWT in the decomposition of image to more definite attributes. This improvement over DWT helps in sharper identification of forged regions within the image during the decomposition and feature extraction stage.

Historically block based techniques have used approximate matching algorithms on the various sub bands or decomposed components of the image. The effectiveness of the technique lies in the better decomposition of the image which can help segregate more definite features of the image so that block matching algorithm can identify them during the comparison of original and suspected forged image. Due to multiple level of filtering SWT offers a much refined decomposition of the input image compared to the conventional DWT based algorithm. Therefore using our proposed approach we have obtained better detection accuracy.

V. RESULT

We have compared the forgery detection result for approaches based on both DWT and SWT algorithms.

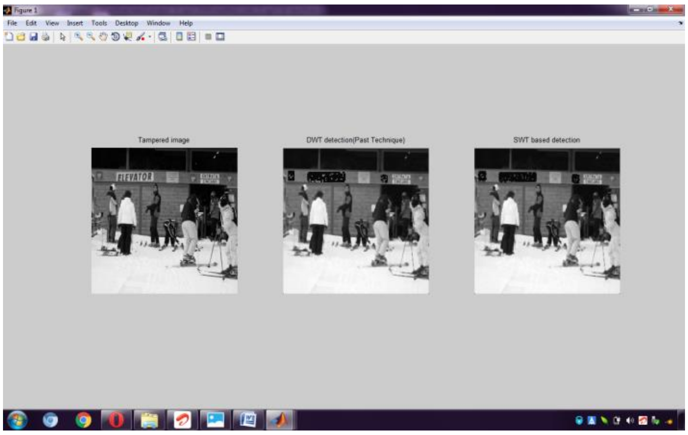
Figure 1
File Edit View Insert Tools Desktop Window Help
Tampered image
DWT detection(Past Technique)
SWT based detection
ELEVATOR

Fig 3. Intermediate results of forgery detection by DWT and SWT

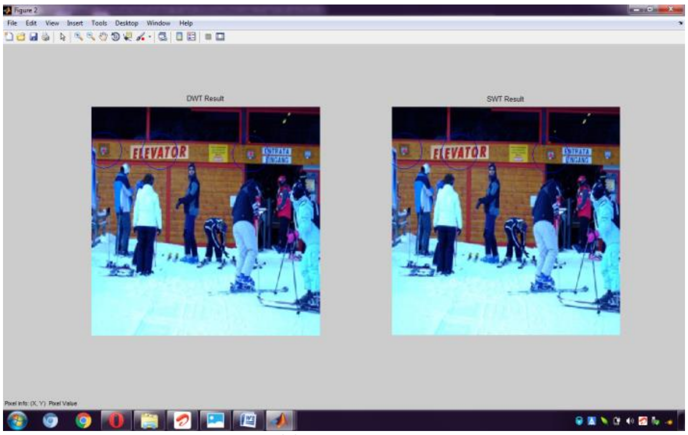
Figure 2
File Edit View Insert Tools Desktop Window Help
DWT Result
SWT Result
ELEVATOR
Pixel info: (X, Y) Pixel Value

Fig 4. Highlighting of forged region by DWT and SWT

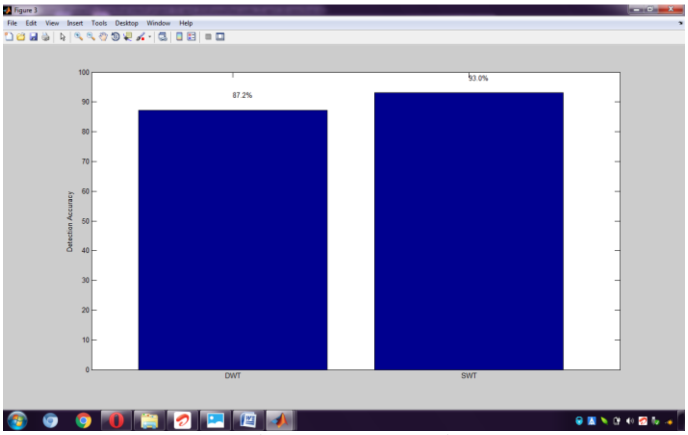

Fig 5. Comparison of detection accuracy of DWT and SWT

We have performed tests across multiple scenarios such as multiple object copy move forgery, mix of copy move and splicing forgery. In all such scenarios the detection accuracy of SWT based technique was higher than that obtained from DWT based technique.

TABLE 1. SUMMARY OF DETECTION ACCURACY OF SWT VS. DWT

Sr. No.	Test case	DWT accuracy	SWT accuracy
1	Copy move forgery – single object	91.72%	97.65%
2	Copy move forgery – multiple objects	92.03%	95.88%
3	Splicing – single object	80.00%	89.97%
4	Splicing – multiple object	78.38%	85.44%
5	Mix of Copy move & Splicing	87.16%	93.02%

VI. CONCLUSION

Digital image forensic is a research area that has gained significant prominence in the past years, owing to increasing need of authenticity of digital images. In this thesis we took a stock of pixel based forensic techniques based on block matching algorithm. While there are many methodologies proposed in this domain, we have preferred to use a refined version of transform – Stationary Wavelet Transform which improves the decomposition of the input image into finer blocks that are subjected to feature extraction. This ability of SWT proves superior over existing techniques based on Discrete Wavelet Transform due to it multiple level filtering algorithm that upsamples and downsamples the inexact coefficients of image into more definite coefficients for the subsequent level. Post the block separation, we are calculate contrast at a smaller block level (4*4) in sequence to establish instance of forgery while comparison in the last stage.

This SWT based technique is stress tested against multiple scenarios of forgery between copy move (single and multiple object forgery) and splicing (single and multiple object composite image) types of forgery. In each of these scenarios SWT based technique has resulted in better detection accuracy compared to the DWT based algorithm. While the computational complexity of the SWT based algorithm is relatively higher than that of DWT, this does not result in any conspicuous extension of processing time or resource requirement even when the forged region within the image is quite large.

ACKNOWLEDGMENT

I take the opportunity to express my cordial gratitude to Ms. Lakshita Landge, Assistant Professor in the Department of Computer Science & Engineering, Astral Institute Of Technology & Research, Indore (M.P.) for the valuable guidance and inspiration throughout the dissertation work. I feel thankful for her innovative ideas, which led to successful completion of this work. I express my gratitude and thanks to all the Director, the Principal and staff members of Computer Science & Engineering department at Astral Institute of Technology & Research for their guidance and cooperation.

REFERENCES

[1] Shivakumar, B.L., Baboo, S.S.: 'Detecting copy-move forgery in digital images: a survey and analysis of current methods', Global J. Computer. Sci. Technol., 2010, 10, pp. 61–65

[2] Shaid, S.Z.M.: 'Estimating optimal block size of copy-move attack detection on highly textured image'. Thesis Submitted to the University of Technology, Malaysia, 2009. Available at http://www.csc.fsksm.utm.my/syed/images/files/publications/thesis/estimating_optimal_block_size_for_copy-move_attack_detection_on_highly_textured_image.pdf

[3] A. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions", Technical Report TR2004-515. Department of Computer Science, Dartmouth College, (2004).

[4] K. XiaoBing and W. ShengMin, "Identifying tampered regions using singular value decomposition in digital image forensics", Proc. Of International conference on computer science and software engineering, (2008), pp. 926–30.

[5] Y. Huang, W. Lu, W. Sun and D. Long, "Improved DCT-based detection of copymove forgery in images", Forensic Sci. Int., vol. 3, (2011), pp. 178–184.

[6] G. Muhammad, M. Hussain and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform", Digital Investigation, vol. 9, (2012), pp. 49–57.

[7] Xufeng Lin, Chang-Tsun Li and Yongjian Hu, "Exposing Image Forgery Through The Detection Of Contrast Enhancement", IEEE Intl. Conf. of Image Processing (ICIP) Sept. 2013.