ISSN 2319 – 7595
Volume 8, No.2, March - April 2019
International Journal of Information Systems and Computer Sciences
Available Online at http://warse.org/IJISCS/static/pdf/file/ijiscs36822019.pdf
https://doi.org/10.30534/ijiscs/2019/36822019

An Effective Method for Detection and Localization of Tampering

Gifty Saju[1], Sreenimol K R[2]
[1]Mangalam College of Engineering, India, sajugifty94@gmail.com
[2]Mangalam College of Engineering, India, sreenimol.kr@mangalam.in

ABSTRACT

Digital transmission of sensitive images and documents over unsecure networks, such as the Internet, has become a general practice. As a result, the digital content has become vulnerable to intentional and unintentional modifications during transmission.
A system that combines linear interpolation for tamper-detection and localization that provide security to exchanged data is the main concern. The algorithm is based on hash based representation of such image and uses discrete wavelet transform method to carry out detection and localization of tampering. And it is robust against harmless manipulation and sensitive enough for even a minute tampering. The proposed model presents a superior tamper detection and recovery capability in comparison to other models in the related literature.

Key words: Image forensic, tampering detection, tampering localization, discrete wavelet transform, image hashing.

1. INTRODUCTION

The interchange and reproduction of digital content has become faster and easier. Such advantages are related with difficulties while guaranteeing digital content trustworthiness check; which are all basic necessities when transmitting specific substance including; formal, legitimate, money related, and religious archive pictures just as therapeutic pictures [1], [2]. In the field of education different tampering techniques give us false information which in turns gives to the delivery of incorrect data to the organization. Students carried out large amount of fraud with their documents for their own advantage. This disturbs the security of the management which is an urgent issue to be comprehended.

These cases emphasize the need for some algorithm or tool to verify, if or not, the suggested content is tampered with. The digital content may apply some operations like contrast enhancement, brightness adjustment etc, in order to increase the quality. These activities are not meant to badly affect the structural component of the image. Such operations are called content preserving manipulation (CPM) and should not be observed as tampering. Any algorithm implemented for tampering detection should be able to avoid such CPMs and identify only the structural tampering.

We use discrete wavelet transform (DWT) [3] as a tool to create the hash representation, it enables us to recognize direction of tampering. The direction of tampering helps us converge quickly on the tampered region in the localized area. This is robust against CPM as well as sensitive for even a minute tampering. In case of multiple tampering, proposed techniques is able to detect location and direction of multiple operations, while some of the existing methods only detect the region of tampering but fail to show the direction. Our proposed technique is quick as it works with littler hash function in comparison with the similar obtained techniques.

2. RELATED WORKS

Fraud tools have become more active nowadays subsequently there is a need to create an algorithm that can detect more complex fraud in digital contents. During transmission, such delicate substance might be intentionally or accidentally manipulated, prompting undesired and even perilous outcomes. In light of this seriousness for protecting sensitive digital content in critical applications, a number of authentication and tamper detection schemes have appeared.

The examination centers around the pixel-based forgery detection techniques[11],[13],[14] since the most common method of tampering digital images are based on pixel-level. This technique can be characterized into four detection categories namely statistical, splicing, resample and copy-move [4],[15]. Copy-move is one of the most commonly used methods among counterfeiters [5],[16]. The copy-move detection methods are classified into two parts mainly keypoint and block based. The advantage in using keypoint is in extracting more robust features. The block based is to reduce image dimensions.

Deepika Sharma, et al. [6],[10] proposed methods based on various techniques for tamper detection. It include principal component analysis (PCA), discrete cosine transform (DCT)[10], discrete wavelet transforms (DWT), singular value decomposition (SVD).

Tushar D. Gadhiya, Anil K. Roy, et al, [7] proposed a method for the detection and localization of tampering by hash based representation and uses discrete wavelet transform. On the other hand, Chun Kiat Tan, et al. [8] propose a fully reversible, dual-layer watermarking scheme with tamper detection capability and locate tampered regions in the images[12].

3. PROPOSED SYSTEM

Figure 1 demonstrates the fundamental advances associated with proposed tampering detection technique. First DWT is applied to digital content which decompose it into four components, then canny edge detector is applied on each

component to abstract edge based feature which are then used to produce hash representation. Canny edge detector [9] is a standout amongst the best existing technique for edge detection.

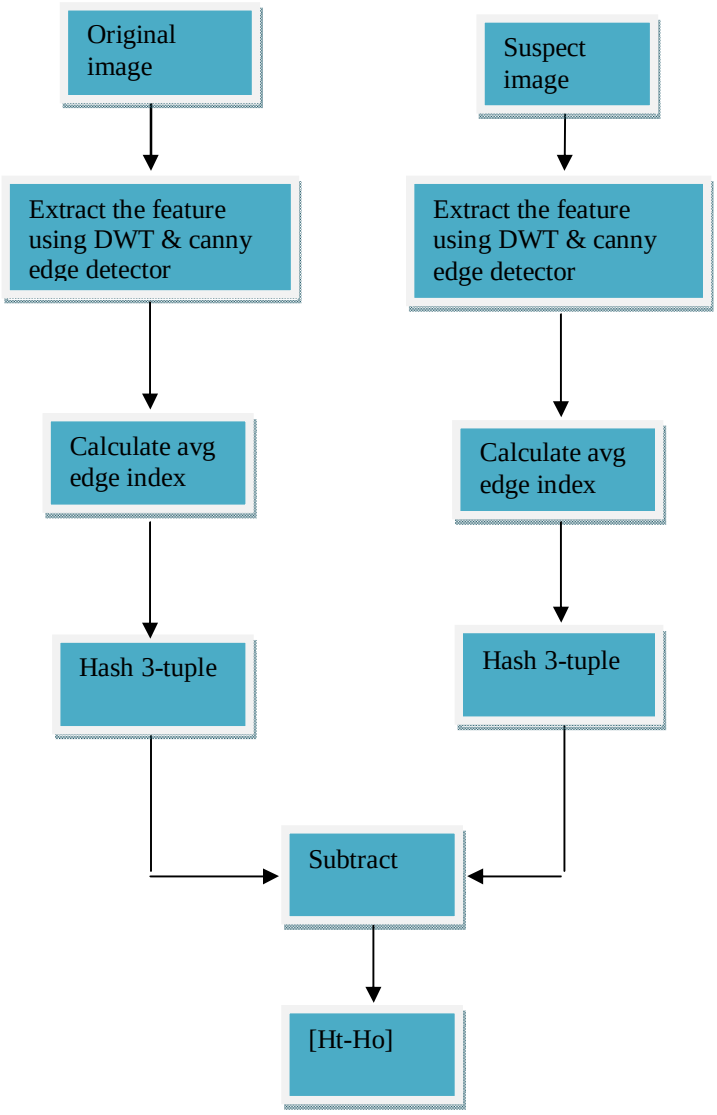

Figure1: Steps involved in proposed technique

Rather than putting away original image we store hash representation of it which is much smaller in size. DWT deteriorates picture into four different components HH (diagonal edge information), HL (horizontal edge information), LH (vertical edge information) and LL (down sampled version of image). The element extricated from 3 segments gives 3- tuple hash values which when put together forms the hash matrix. Hash matrices of suspect and original images when subtracted, results the tampered region. Tampering is thus identified in every one of the three directions namely vertical, horizontal and diagonal.

As we probably aware, edges convey the most essential basic data of a picture. Any structural tampering done in the image with malevolent aim will think about the edges as it were. Therefore we used only three components that contain edge information HL, LH and HH directions, and we disregard the fourth component i.e., LL. Canny edge detector is applied to sharpen edges recognized by DWT. Canny edge detector results edge pixels represented by the value 1 and no edge pixel represented by value 0.

Hash Generation is applied on all three components which gives hash tuple (HLH, HHL, HHH), where

HLH -> Hash matrix of LH component
HHL-> Hash matrix of HL component
HHH-> Hash matrix of HH component

Let the hash tuple of original image be (HLH_{org}, HHL_{org}, HHH_{org}) and hash tuple for the suspect image be (HLH_{sus}, HHL_{sus}, HHH_{sus}). Difference of two hash matrices in tuple form (ΔHLH, ΔHHL, ΔHHH) is found where:

$$\Delta HLH = HLH_{org} - HLH_{sus}$$
$$\Delta HHL = HHL_{org} - HHL_{sus}$$
$$\Delta HHH = HHH_{org} - HHH_{sus}$$

4. RESULT

To check robustness of the technique we took 30 images for analyze and performed different CPM operations like brightness change, contrast enhancement, gamma correction, double JPEG compression etc. using adjustment function of adobe Photoshop. The average edge index of manipulated and original images was compared.

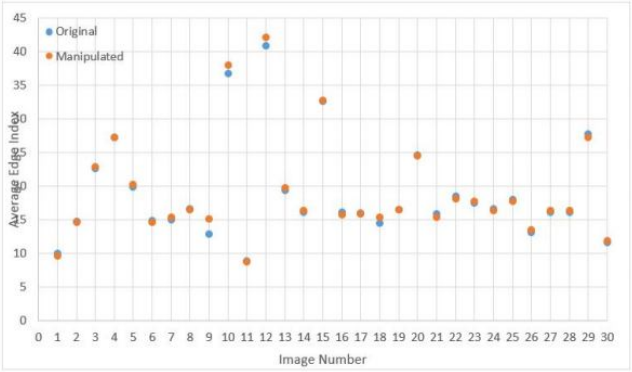

Figure 2: Effect of harmless manipulation on average edge index, HL component of the image.

Figure 2 shows result given by the proposed strategy where the tampered image was generated by adding hairline fracture in different direction into image. As we can see localization of tampering was attained by subtracting hash tuple and by considering similarity value of each component of hash tuple we can determine the direction of tampering.

5. CONCLUSION

Our algorithm has been proposed to achieve high integrity and authenticity. This technique can detect and localize tampering in a digital document image. A minute tampering in form of a thin line may cause diagnosis turn to a different direction. Such tampering may result into heavy losses to insurance companies. Discrete wavelet transform method fits well with this requirement. Because of tuple-nature of hash function, it identifies and localizes exactly where the tampering is done.

The algorithm not only consumes less computational resource but also as robust and sensitive as required by the basic properties of hash function representing a digital image. By building the database of such digital certificate images, documents can have the confidence that the fraudulent claims of the nature would be drastically reduced in near future.

REFERENCES

1. S. Barrett, **Insurance fraud and abuse: A very serious problem**, May 2017K. Young. **Internet addiction: the emergence of a new clinical disorder, Cyberpsychol**. Behav., 1998.
2. S. H.-H. William J Rudman, **Healthcare fraud and abuse.** May 2017.
3. L. Starck, F. Murtagh, and J. M. Fadili, **Sparse image and signal processing: wavelets, curvelets, morphological diversity**. Cambridge University Press, 2010. https://doi.org/10.1017/CBO9780511730344
4. S. A. Chatzichristofis, K. Zagoris, Y. S. Boutalis, and N. Papamarkos, **Accurate Image Retrieval Based on Compact Composite Descriptors and Relevance Feedback Information,** International Journal of Pattern Recognition and Artificial Intelligence, 2010. https://doi.org/10.1142/S0218001410007890
5. P. Kakar and N. Sudha, **Exposing Postprocessed Copy-Paste Forgeries through Transform-Invariant Features,** on Information Forensics and Security, 2009.
6. Deepika Sharma, Pawanesh Abrol, **Digital Image Tampering – A Threat to Security Management,** IJRCCE October 2013.
7. Tushar D. Gadhiya, Anil K. Roy, Suman K. Mitra and Vinod Mall, **Use of Discrete Wavelet Transform Method for Detection and Localization of Tampering in a Digital Medical Image,** 2017 IEEE https://doi.org/10.1109/TENCONSpring.2017.8070082
8. Chun Kiat Tan, Jason Changwei Ng, Xiaotian Xu, **Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability,** Journal of Digital Imaging 2011
9. J. Canny, **A computational approach to edge detection,** Pattern Analysis and Machine Intelligence, IEEE 1986. https://doi.org/10.1109/TPAMI.1986.4767851
10. S. Kumar, J. Desai, and S. Mukherjee, **A fast DCT based method for copy move forgery detection, in Image Information Processing (ICIIP),** 2013 IEEE https://doi.org/10.1109/ICIIP.2013.6707675
11. I. Amerini, L. Ballan, R. Caldelli, A. Bimbo, and G. Serra, **"A sift-based forensic method for copy–move attack detection and transformation recovery,"** on Information Forensics and Security, 2011. https://doi.org/10.1109/TIFS.2011.2129512
12. X. Pan and S. Lyu, **Detecting image region duplication using SIFT features,** in ICASSP, 2010. https://doi.org/10.1109/ICASSP.2010.5495482
13. M. Ghorbani, M. Firouzmand, and A. Faraahi, **DWT-DCT (QCD) based copy-move image forgery detection,** in Systems, Signals and Image Processing (IWSSIP), 2011
14. M. Shabanifard, M. G. Shayesteh, and M. A. Akhaee, **Forensic Detection of Image Manipulation Using the Zernike Moments and Pixel-Pair Histogram,** 2013. https://doi.org/10.1049/iet-ipr.2012.0717
15. K. Sunil, D. Jagan, and M. Shaktidev, **DCT-PCA based method for copy-move forgery detection,** Computer Society of India, 2014. https://doi.org/10.1007/978-3-319-03095-1_62
16. K. Li, C. Xiao-ping, L. Li, S. Li, H. Zhu, S. C. Chu, et al., **Copy-Move Forgery Detection in Digital Image,** CISP, 2013.