Use of Discrete Wavelet Transform Method for Detection and Localization of Tampering in a Digital Medical Image

Tushar D. Gadhiya, Anil K. Roy, Suman K. Mitra and Vinod Mall
Dhirubhai Ambani Institute of Information and Communication Technology, Gandhinagar.

***Abstract*—Use of digital images has increased tremendously in medical science and with that has increased the query on authenticity of the image. Authenticity of the digital image is very important in the area of scientific research, forensic investigations, government documents, etc. With the help of powerful and user friendly image editing software like Microsoft Paint and Photoshop it became extremely easy to tamper with a digital image for malicious objective. Of late this problem has been encountered in medical imaging also for the purpose of fake insurance claims. We propose an algorithm to address this problem by which one can detect and localize tampering in a digital medical image. This algorithm is based on hash based representation of such image and uses discrete wavelet transform method to carry out detection and localization of tampering. We will show that our algorithm is robust against harmless manipulation and sensitive enough for even a minute tampering. Our proposed technique consumes less resource as it works with smaller hash function in comparison with the similar available techniques.**

***Index Terms*—Image forensic, image hashing, discrete wavelet transform, tampering detection, tampering localization.**

I. Introduction

USE of digital radiography as compared to the conventional radiography has increased in recent years because it can be produced even with lower exposure to the radiation. Development of the radiograph takes less time. Also the chances of error in radiograph are extremely rare. But unfortunately there is no way that could protect images against tampering and could ensure its authenticity. This makes digital radiography images vulnerable to changes which may be applied to them with malicious intention.

Reports [1], [2] say that alone Medicare lost nearly $12 billion to fraudulent or unnecessary claims. Recent studies show [3], [4], [5], [6] that manipulation in radiographs is a serious issue and can be used in illegal claim of medical insurance of a patient or publishing fraud result. It has been shown [7] that one can claim the medical insurance by simply tampering with the patient's radiograph. Many of fraud claims go unnoticed because, as of now, insurance companies do not have any standard tool that can verify the authenticity of the radiographs that are submitted in support of the claim.

Almost similar challenge prevails in the area of publication of research results in medical science. The human stem cell related breaking news published by Hwang [8] was one such notorious case that shook the whole medical science research community. The investigating committee immediately came up with some guidelines [9] that should be followed by research journal publications in order to verify the authenticity of all the digital images submitted in support of the claims by author(s). Another case, in the area of cell biology [10], also exposes similar unethical and illegal practice seen in medical science.

These cases highlight the need for some algorithm or tool to verify, if or not, the submitted image is tampered with. After taking a radiograph, the radiologist may apply some operations like brightness adjustment, contrast enhancement etc. in order to improve the quality of the image. These operations are not intended to adversely affect the structural component of the image. Such operations are called content preserving manipulation (CPM) and should not be considered as tampering. Any algorithm designed for tampering detection should be able to ignore such CPMs and detect only the structural tampering.

There are mainly two categories of tampering detection techniques. The first category is called Blind Technique. The methods falling into this type of technique use no prior information about the original image. The second category is called Non-blind Technique in which either we have an original image or we have some mathematical representation of the original image. In case of non-blind technique, watermarking [11], [12], [13] and hash function [14], [15], [16], [17] methods are two main approaches. As we know any harmful tampering done with a digital image will affect structural content of the image, researchers are trying to come up with different methods to extract structural content of the image and use it to generate mathematical representation of the image. One such method to extract structural content of the image is from the luminance value of the image [18]. Method proposed in [17] is a two-step method, first step extracts features from the image and the second compresses those features to generate hash matrix.

Hash function is basically a binary string which can efficiently represent features of the image. Any hash function based algorithm should satisfy the following four properties:

1) **Sensitivity:** Algorithm should be able to identify any minor tampering in a digital image.
2) **Robustness:** Algorithm should be able to ignore harmless manipulations or CPMs such as JPEG compression,

978-1-5090-6255-3/17/$31.00

contrast enhancement and blurring etc.

3) **Low collision probability:** Probability of two images getting same hash function should be extremely small.
4) **Compact size:** Size of the hash function should be as small as possible and it should contain maximum possible information about the image.

As we know that edges present in an image can represent its structural content very efficiently, method proposed in [19] exploits this idea. They use canny edge detector [20] to find edges in the image which is used to calculate Average Edge Index [19] to generate a hash matrix. Robust algorithm should be able to ignore CPM. However, repeated CPMs on the same image may amount to structural tampering. For example, blurring operation will not affect an edge significantly but when repeated a number of times may remove weak edges from the image. Motivation behind this algorithm is to identify even the minutest tampering as clearly as possible.

We use discrete wavelet transform (DWT) [21] as a tool to generate the hash representation, it allows us to identify direction of tampering. The direction of tampering helps us converge quickly on the tampered region in the localized area. We will show that our algorithm is robust against CPM as well as sensitive for even a minute tampering. In case of multiple tampering, proposed method is able to identify location and direction of multiple operations, while some of the existing methods only identify the region of tampering but fail to show the direction. Our proposed technique is fast as it works with smaller hash function in comparison with the similar available techniques.

II. Proposed Method

Fig. 1 shows the basic steps involved in proposed tampering detection technique. First DWT is applied to image which decompose it into four components, then canny edge detector is applied on each component to extract edge based feature which are then used to generate hash representation using algorithm discussed later. Instead of storing original image we store hash representation of it which is much smaller in size.

DWT decomposes image into four different components HH, HL, LH and LL, where HL component contains horizontal edge information, LH component contains vertical edge information, HH component contains diagonal edge information and LL component is a down sampled version of image. Canny edge detector is then used to extract edges from those components. So, if there is a particular direction specific tampering in an image then it will be reflected in the respective component. The feature extracted from 3 components gives 3-tuple hash values which when put together forms the hash matrix. Hash matrices of original and suspect images when subtracted, gives the tampered region. Tampering is thus detected in all three directions namely vertical, horizontal and diagonal.

Canny edge detector [20] is one of the best existing method for edge detection.Steps involved in canny edge detector is as follows. First input image is smoothened by applying a Gaussian filter to remove noise from the image. Then gradients at each pixel are calculated by using Sobel-operator followed by non-maximum suppression to sharpen the edges. Non-maximum suppression preserves local maxima and removes everything else. After this, double thresholding mechanism is used to remove false edges. The last step of canny edge detector is edge tracking by hysteresis. In this step, strong edges are directly included into the output image because strong edges are most probably are the true edges while weak edges can be true edges or it can be because of the noise. So the weak edge connected with the strong edge will be included into the output image.

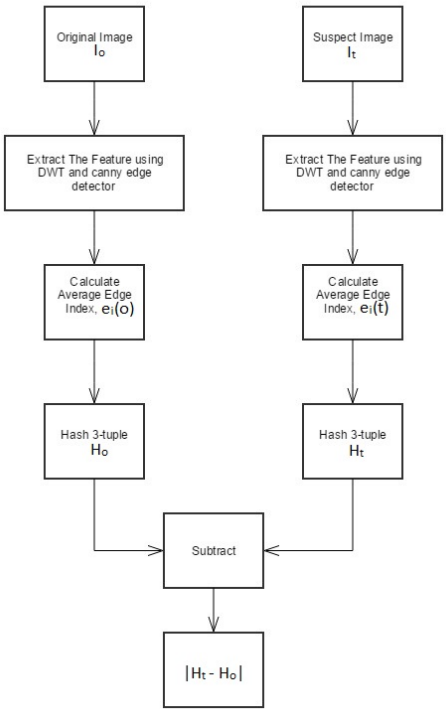

Fig. 1. Steps involved in proposed algorithm.

A. Hash tuple generation algorithm:

DWT is applied on the suspect image which decomposes it into four different components. As we know, edges carry the most important structural information of an image. Any structural tampering done in the image with malicious intention will reflect on the edges only. Therefore we used only three components that contain edge information in horizontal (HL), vertical (LH) and diagonal (HH) directions, and we ignored the fourth component i.e., LL. Canny edge detector is applied to sharpen edges detected by DWT. Result of canny edge detector has edge pixels represented by the value 1 and non-edge pixel represented by value 0. Hash Generation algorithm is applied on all three components which gives hash tuple (H_{LH}, H_{HL}, H_{HH}) as shown in equation 1, where H_{LH} is a

Algorithm 1 Hash Generation

procedure GENERATE HASH
  $I \leftarrow$ *input image*
  $M \leftarrow$ *number of rows*
  $N \leftarrow$ *number of columns*
  $q \leftarrow$ *size of block*
  $t_1 \leftarrow \lceil \frac{2M}{q} - 1 \rceil$
  $t_2 \leftarrow \lceil \frac{2N}{q} - 1 \rceil$
  for `each block in I` **do**
    for $i \in \{1, ..., t_1\}$ **do**
      for $j \in \{1, ..., t_2\}$ **do**
        $P_{ij} = \frac{\sum_{l=1,m=1}^{l=q,m=q} X_{lm}}{q^2}$
  for $i \in \{1, ..., t_1\}$ **do**
    for $j \in \{1, ..., t_2\}$ **do**
      $H_{ij} = P_{i-1,j} + P_{i,j-1} + P_{i,j} + P_{i+1,j} + P_{i,j+1}$
  return H

hash matrix of LH component H_{HL} is a hash matrix of HL component and H_{HH} is a hash matrix of HH component.

$$\begin{bmatrix} H_{LH_{11}}, H_{HL_{11}}, H_{HH_{11}} & H_{LH_{12}}, H_{HL_{12}}, H_{HH_{12}} & \cdots & H_{LH_{1t_1}}, H_{HL_{1t_1}}, H_{HH_{1t_1}} \\ H_{LH_{21}}, H_{HL_{21}}, H_{HH_{21}} & H_{LH_{22}}, H_{HL_{22}}, H_{HH_{22}} & \cdots & H_{LH_{2t_1}}, H_{HL_{2t_1}}, H_{HH_{2t_1}} \\ \vdots & \vdots & \ddots & \vdots \\ H_{LH_{t_21}}, H_{HL_{t_21}}, H_{HH_{t_21}} & H_{LH_{t_22}}, H_{HL_{t_22}}, H_{HH_{t_22}} & \cdots & H_{LH_{t_2t_1}}, H_{HL_{t_2t_1}}, H_{HH_{t_2t_1}} \end{bmatrix} \quad (1)$$

B. Localization of Tampering:

Let the hash tuple of original image be $(H_{LH_{org}}, H_{HL_{org}}, H_{HH_{org}})$ and hash tuple for the suspect image be $(H_{LH_{sus}}, H_{HL_{sus}}, H_{HH_{sus}})$. Difference of two hash matrices in tuple form $(\Delta H_{LH}, \Delta H_{HL}, \Delta H_{HH})$ is found where:

$$\Delta H_{LH} = H_{LH_{org}} - H_{LH_{sus}} \quad (2)$$

$$\Delta H_{HL} = H_{HL_{org}} - H_{HL_{sus}} \quad (3)$$

$$\Delta H_{HH} = H_{HH_{org}} - H_{HH_{sus}} \quad (4)$$

The three matrices ΔH_{LH}, ΔH_{HL}, ΔH_{HH} give accurate description about the tampered regions in respective directions. If tampering done is in only one direction, for example diagonal direction, then only H_{HH} component will get affected, other two component will not be affected. So the tampering is detected only in ΔH_{HH} matrix. This demonstrates that by analyzing component of hash tuple difference we can identify the direction of tampering.

III. EXPERIMENT

To create a database, we collected around 100 digital radiographs of size 1954 x 2410 from a hospital which contain bone x-rays of different parts of the body. Tampering in the image was done using Adobe Photoshop CS6.

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

Obtained results are shown in the Fig. 2 for image of size 1954×2410. The sampling block size used was 50×50. One finds that change in Average Edge Index is negligible for various CPMs. So, it can be concluded that hash function is robust against content preserving manipulation.

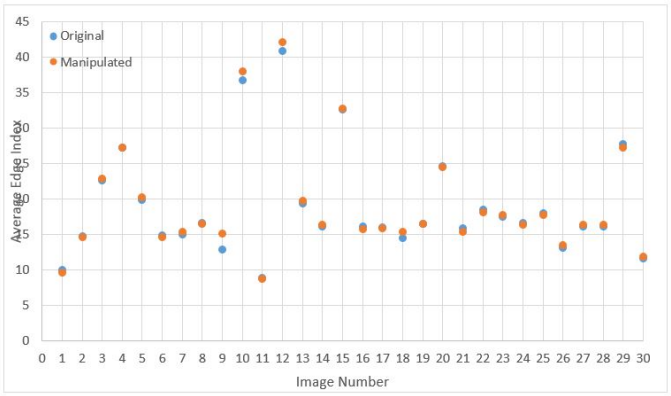

Fig. 2. Effect of harmless manipulation on average edge index of HL component of the image.

The advantage of applying DWT technique is that the algorithm consumes less computational resource. The reason being that we have to process only $3/4^{th}$ part of wavelet transformed image. Therefore the proposed algorithm is faster and the size of the hash matrix generated by the algorithm is smaller in comparison to one of the existing methods [19]. In this method authors have calculated an average edge index using Canny Edge Detector and hence identified as well as localized tampering in a digital image in non-blind case. Difference in improvement might not be visible for smaller images but as we increase size of the image, improvement can be seen clearly.

We used Similarity Value [16] to determine how much similar two hash matrices are. If the similarity value is close to 1 then two hash matrices are very similar and if the similarity value is close to zero, the two hash matrices are very different. For exactly same two hash matrices, similarity value will be 1.

If there exists multiple tampering in the image and the locations of the tampering are very close then earlier method [19] may not be able to differentiate these multiple tampering operations. Proposed algorithm can differentiate multiple tampering present even in a very close location by analyzing hash tuple difference as explained in previous section. The same is demonstrated in Figs. 3 and 4. This result shows that while the existing method can give the location of the tampering, our method gives more precise localization of the image tampering.

Table I shows result obtained by the proposed method where the tampered image was generated by adding hairline fracture in different direction into image. As we can see localization of tampering was achieved by subtracting hash tuple and

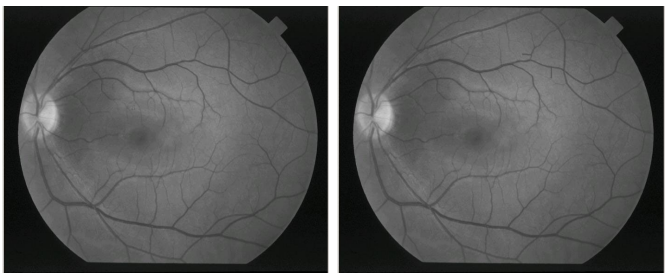

Fig. 3. (a) Original image of retina. (b) Tampered image of retina.

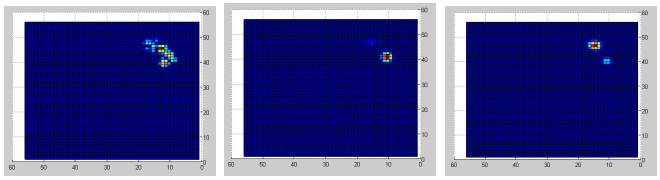

Fig. 4. (a) Localization using existing method [19]. (b) Localization in LH component of our proposed method. (c) Localization in HL component of our proposed method.

direction of tampering was determined by similarity value of each component of hash tuple.

IV. Conclusion

Medical images are different from other types of images as these are very sensitive. They tell about condition of internal organs which are not seen by eyes. Hence integrity and authenticity of the image can not be verified visually. Also, even 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. Therefore, handling of medical images needs special attention.

Our algorithm using 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. This was not possible in earlier algorithms. In the non-blind case, if the insurance company asks for the hash function of the medical image of a particular patient, it may be obtained from the hospital or from the radiologist and then the two images can be compared for the possibility of malicious tampering with the original image. Our algorithm can be proved very useful for X-ray images of fractured bones, ligament problem, dental treatment and root canaling, retinal treatment and eye surgery, CT scans and many more similar radiograph based treatments.

It has also been discussed that the proposed algorithm not only consumes less computational resource but also is as robust and sensitive as required by the basic properties of hash function representing a digital image. We hope that by building the database of such digital radiograph images, insurance companies can have the confidence that the fraudulent claims of the nature discussed in paper would be drastically reduced in near future.

References

[1] S. Barrett, "Insurance fraud and abuse: A very serious problem." https://www.quackwatch.org/02ConsumerProtection/insfraud.html, May 2017.

[2] S. H.-H. William J Rudman, "Healthcare fraud and abuse." https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2804462/, May 2017.

[3] F. L. Calberson, G. M. Hommez, and R. J. De Moor, "Fraudulent use of digital radiography: methods to detect and protect digital radiographs," *Journal of endodontics*, vol. 34, no. 5, pp. 530–536, 2008.

[4] A. Chowdhry, K. Sircar, D. B. Popli, and A. Tandon, "Image manipulation: Fraudulence in digital dental records: Study and review," *Journal of forensic dental sciences*, vol. 6, no. 1, p. 31, 2014.

[5] K. P. Singbal, N. Chhabra, and B. Madan, "Digital imagery: reality or fakery," *International Journal of Contemporary Dentistry*, vol. 1, no. 3, 2011.

[6] M. L. Richardson, M. S. Frank, and E. J. Stern, "Digital image manipulation: what constitutes acceptable alteration of a radiologic image?," *American journal of roentgenology (AJR)*, vol. 164, no. 1, pp. 228–229, 1995.

[7] A. Tsang, D. Sweet, and R. E. Wood, "Potential for fraudulent use of digital radiography," *The Journal of the American Dental Association*, vol. 130, no. 9, pp. 1325–1329, 1999.

[8] D. Cyranoski, "Verdict: Hwang's human stem cells were all fakes," *Nature*, vol. 439, no. 7073, pp. 122–123, 2006.

[9] I. Fuyuno and D. Cyranoski, "Doubts over biochemist's data expose holes in japanese fraud laws," *Nature*, vol. 439, no. 7076, pp. 514–514, 2006.

[10] H. Pearson, "Image manipulation: Csi: cell biology," *Nature*, vol. 434, no. 7036, pp. 952–953, 2005.

[11] F. Khelifi and J. Jiang, "Perceptual image hashing based on virtual watermark detection," *Image Processing, IEEE Transactions on*, vol. 19, pp. 981–994, April 2010.

[12] J. Fridrich and M. Goljan, "Robust hash functions for digital watermarking," in *Information Technology: Coding and Computing, 2000. Proceedings. International Conference on*, pp. 178–183, 2000.

[13] Z. Guojuan and L. Dianji, "An overview of digital watermarking in image forensics," in *Computational Sciences and Optimization (CSO), 2011 Fourth International Joint Conference on*, pp. 332–335, April 2011.

[14] F. Lefebvre, J. Czyz, and B. Macq, "A robust soft hash algorithm for digital image signature," in *Image Processing, 2003. ICIP 2003. Proceedings. 2003 International Conference on*, vol. 2, pp. 495–498, Sept 2003.

[15] R. Venkatesan, S.-M. Koon, M. Jakubowski, and P. Moulin, "Robust image hashing," in *Image Processing, 2000. Proceedings. 2000 International Conference on*, vol. 3, pp. 664–666 vol.3, 2000.

[16] V. Mall, A. Roy, S. Mitra, and K. Bhatt, "Non-blind method of detection and localization of structural tampering using robust hash-like function and similarity metric for digital images," in *TENCON 2012 - 2012 IEEE Region 10 Conference*, pp. 1–6, Nov 2012.

[17] V. Monga and B. Evans, "Perceptual image hashing via feature points: Performance evaluation and tradeoffs," *Image Processing, IEEE Transactions on*, vol. 15, pp. 3452–3465, Nov 2006.

[18] V. Mall, K. Bhatt, S. Mitra, and A. Roy, "Exposing structural tampering in digital images," in *Signal Processing, Computing and Control (ISPCC), 2012 IEEE International Conference on*, pp. 1–6, March 2012.

[19] V. Mall, A. Roy, S. Mitra, and S. Shukla, "Detection of structural tampering in a digital image using canny edge detector," in *Informatics, Electronics Vision (ICIEV), 2013 International Conference on*, pp. 1–7, May 2013.

[20] J. Canny, "A computational approach to edge detection," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. PAMI-8, pp. 679–698, Nov 1986.

[21] J.-L. Starck, F. Murtagh, and J. M. Fadili, *Sparse image and signal processing: wavelets, curvelets, morphological diversity*. Cambridge University Press, 2010.

No.	Original Image	Tampered Image	Localization	Similarity Value of HH Compo-nent	Similarity Value of HL Compo-nent	Similarity Value of LH Compo-nent
1				1	1	0.5326
2				1	0.8704	1
3				0.7603	1	1
4				1	1	0.2902
5				1	0.4735	1
6				1	1	0.8003

TABLE I

LOCALIZATION OF TAMPERING USING BLOCK SIZE OF 50X50 AND EFFECT OF TAMPERING ON SIMILARITY VALUE IN AN IMAGE.