Image Splicing Forgery Detection Using Local Binary Pattern and Shift Vector

Mohanad F. Jwaid Al-Husseinawi[1], Husam K. Salih[2], Saif A. Salim[3], Ahmed Q. Mohammed[4]

[1, 2]Maharashtra Institute of Technology, Information Technology, Pune, India

[3, 4]Dr. DY Patil Institute of Technology, Department of Computer, Pune, India

Abstract: ***Digital images are the simple and fast way of communication. It can convey huge information in short time. But In our now life days various tools and application are available that manipulates the image without leaving any trace of tampering. So we need to design a system to detect the forged image. There are two types of image forgery first one is copy-move and second one is Image splicing. In this paper will base on the splicing image, and the proposed system will utilize Local Binary Pattern and Shift Vector techniques. The required steps to detect the forgery are pre-processing, feature extraction, feature matching.***

Keywords: Digital image, Splicing image, LBP, Shift Vector

1. Introduction

In our time, digital image plays a significant part in our life. It being used as a means of pictorial information in everyday newspapers and magazines as a proof in courts of law, and in the medical diagnose field [1]. On the other hand, there are an advanced of great image processing tools, anyone can easily modification a real picture and generate a fake image. Photoshop, GIMP, PAINT COREL are an example of such an editing tools which can do an alteration in digital images by changing chunks of an image without leaving the special effects of the modification in the fake image. These changes cannot be discovered through human eyes. The image fakes can hide or add a significant piece in an original image to misguide the court of law [2]. There are two methods of image forgery, passive and active approach, where passive method contain image splicing and copy-move image. The active method contain digital signature and watermarking. Image splicing is one of the most common kinds of image tampering [3]. There are many techniques utilized for discovery image forgery as: discrete wavelet transform, principle component analysis, discrete cosine transform, Singular Value Decomposition, Scale Invariant Feature Transformation and Locally Linear Embedding. In this paper will base on LBP, shift vector techniques. There is an urgent need to design an image forgery detection system in various fields of Forensic investigation, Criminal investigation, insurance processing, Surveillance systems, Intelligence services, Medical imaging and Journalism. Next figures will present image forgery types.

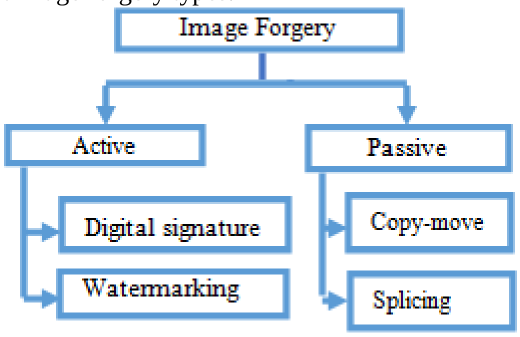


Figure 1: Image forgery types

2. Image Splicing

Image splicing is a common kind to make a tampered image where a section from one image is copied and pasted into another image which products composite picture called spliced image; cut and join two or more snaps of pictures [2]. This type of fake is a challenging issue from tamper detection point of view. The complicated forgery may include some post-processing like blurring, JPEG compression, etc. [4]. That performs the forgery detection very hard. Many researchers tend to discover techniques that discover this kind of forgery. There are various methods to discover such an alteration, some of them dependent on the format of the image Figure 2 shows one of the example of image splicing process.

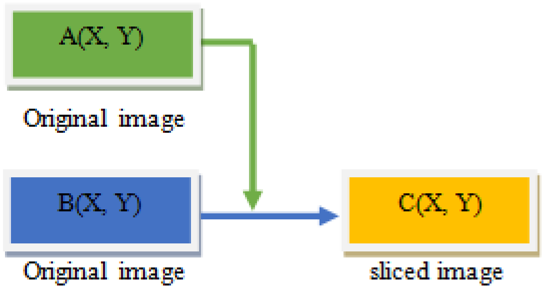


Figure 2: Steps to create image splicing

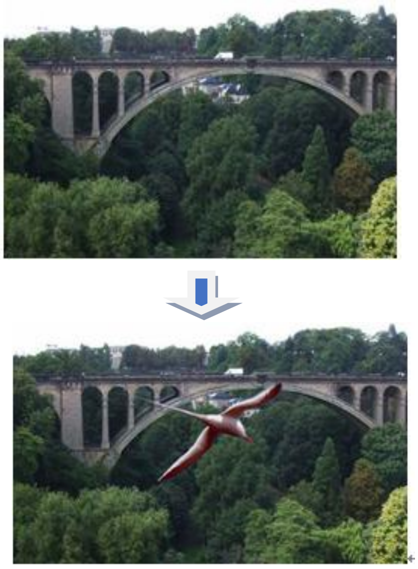


Figure 3: Example of image splicing

3. Proposed Algorithm

To detect the splicing forgery image, we must to apply four steps: pre-processing, feature extraction, feature matching then Post-processing

3.1 Convert RGB to YCbCr

In this step we change the colour of an input image from R, G, B (red, green, blue) to the YCbCr colour. First thing we need to know what the meaning of RGB. Image is stored in the memory as values of pixels, each pixel include three bytes, and each bytes include eight bits. So the total values is equal to 16 million colour in each pixel.

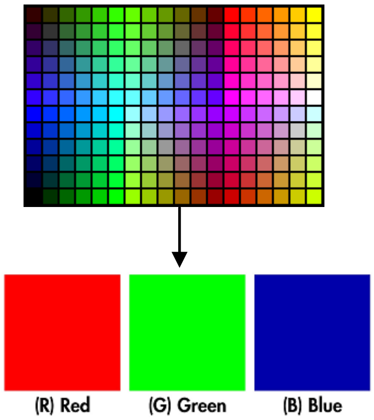


Figure 4: RGB colour

While YCbCr Contain the color information and they can be highly compressed. It is include two parts, Luminance and Chrominance. This paper based on the Chrominance, because the human eyes are less sensitive to chrominance than luminance.

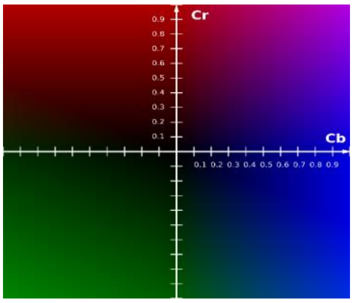


Figure 5: YCbCr colour

To extract YCbCr from R, G, and B, we need to apply:

$$Y = 0.299R + 0.587G + 0.114B \text{ .... } (1)$$

$$Cr = 0.701R - 0.587G - 0.114B \text{ .... } (2)$$

$$Cb = -0.299R - 0.587G + 0.886B \text{ .... } (3)$$

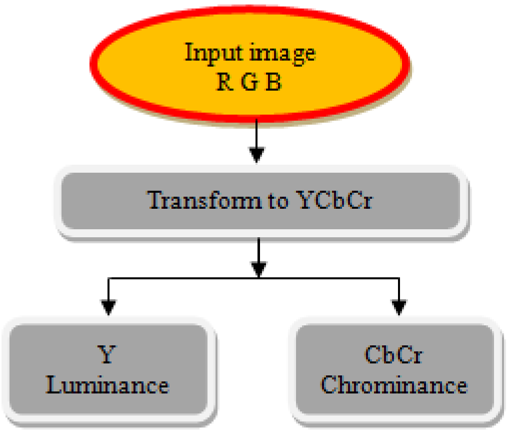


Figure 6: Pre-processing

After pre-processing, input image will dividing into overlapping block.

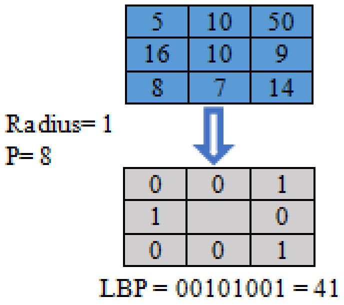
3.2 *Apply LBP*

In feature extraction, we utilize Local Binary Pattern. Where LBP is a powerful feature for texture classification which has been used widely in this manner. LBP computed by apply:

$$\text{LBPp.r} = \sum_{i=0}^{p-1} s(Pi - Pc)2^{i} \quad \text{........ } (4)$$

$$\text{S (Pi-Pc)} = \begin{cases} 1 \; Pi - Pc \geq 0 \\ 0 \; Pi - Pc \leq 0 \end{cases} \quad \text{... } (5)$$

Where p_c is the gray value of the center pixel and p_i represents eight neighbouring pixels. If p_i is smaller than p_c, then the binary result of the pixel is set to 0; otherwise, it is set to 1.



5	10	50
16	10	9
8	7	14

Radius= 1
P= 8

0	0	1
1		0
0	0	1

LBP = 00101001 = 41

Figure: 7 computing the original LBP code

After feature extraction step, blocks with similar feature vectors must be identified, and exact copied blocks are determined based upon some criteria. To implement this method, the feature vectors are lexicographically sorted and similar vectors are determined to specify the forgery.

3.3 Apply Shift vector

In this step we match between the points of images to select if the upload image is original or forgery. Shift vector is utilize in this step. Let (x1, x2) and (y1, y2) be the locations of two similar blocks. The shift vector between blocks can be computed as in:

$$Sh = (sh1, sh2) = (x1\text{-}y1), (x2\text{-}y2) \text{ .... } (6)$$

−Sh and Sh, both shift vectors represents same shifting so they can be normalized. If required, shift vector is multiplied with −1 such that sh1 ≥ 0. Counter value k of normalized shift vector increased block pair with same shifting is detected.

$$K\ (Sh1, Sh2) = k\ (Sh1, Sh2) +1 \text{ .... } (7)$$

Firstly, counter value is set as zero. When this method complete, counter value displays frequency of occurrence of different shift vectors corresponding to matching chunks. A threshold is set for occurrence of normalized shift. $Sh^{(1)}$, $Sh^{(2)}$, $Sh^{(n)}$. If threshold value is great then some matching blocks will be detected as non-match. For minor value of threshold too a lot of incorrect matches will happen.

With shift vectors, matched blocks are discovered. Blocks with similar shifting are characterized with different colour to display fake section of input duplicate.

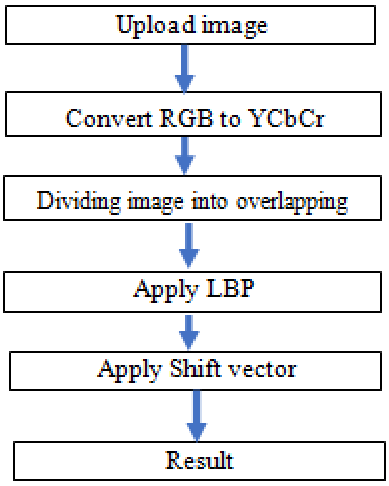


Figure 8: Proposed system architecture

4. Experimental Result

The upload image of the proposed system is being taken from CASIA dataset. CASIA ITDE V1.0, it is collected an image set containing 1,721 color images of size 384 _ 256 pixels with JPEG format. It divided these images into two subsets: authentic set and tampered set. There are 800 images in the authentic set and 921 images in the tampered set. The proposed system is based on two parameters:

$$T_{PR} = \frac{\textit{Image detected as forged being forged}}{\textit{Original image}} \text{....... } (8)$$

$$F_{PR} = \frac{\textit{Image detected as forged being original}}{\textit{Original image}} \text{... } (9)$$

Table 1: Average detection rate

Method	T_{PR} %	F_{PR} %
Yu-Feng Hsu and Shih-Fu Chang [7]	70	9
X.Pan, and S.Lyu [6]	83	8.8
Thibaut Julliand_, Vincent Nozick † and Hugues Talbot [8]	84	5.9
The proposed method	89	8

5. Conclusion

The meaning of image forgery detection discussed in this paper, there are two types of forgery. The common types of forgery is splicing image. The proposed method started with divide the chrominance of input image into overlapping blocks. Then Local Binary Pattern utilized in feature extraction. In the feature, matching applied shift vector. The input image is taken from CASIA V1. The accuracy is achieved to 89 % and the percent of false is decreased to 8%.

References

[1] Bayram S., Avcibas I., Sankur, and B. Memon N., “Image manipulation detection,” Journal of Electronic Imaging – October - December 2006 – Volume 15, Issue 4, 041102 (17 pages), vol. 15(4), 2006.

[2] Sencar H. T. Memon N. Sutcu Y., Coskun B., “Tamper detection based on regularity of wavelet transform coefficients,” *Proc. ICIP, International Conference on Image Processing*, 2007.

[3] T. J. De Carvalho, C. Riess, E. Angelopoulou, H. Pedrini, and A. D. R. Rocha, “Exposing digital image forgeries by illumination color classification,” *IEEE Trans. Inf. Forensics Secur., vol. 8, no. 7, pp. 1182–1194, 2013*

[4] P. Zhang, and X. Kong, “Detecting image tampering using feature fusion,” In Proc. *International Conference on Availability, Reliability, and Security, ARES, pp. 335–340, 2009.*

[5] Y.-F. Hsu and S.-F. Chang, “Detecting image splicing using geometry invariants and camera characteristics consistency”, IEEE ICME, July 2006.

[6] X.Pan, and S.Lyu, Member, "Region Duplication Detection Using Image Feature Matching", *IEEE transactions on information forensics and security, vol. 5, no. 4, december 2010*

[7] Yu-Feng Hsu and Shih-Fu Chang, “image splicing detection using camera response function consistency and automatic segmentation”, *IEEE*, ICME 2007

[8] Thibaut Julliand, Vincent Nozick, Hugues Talbot, “Automated Image Splicing Detection from Noise Estimation in Raw Images”, 2017

[9] B. Mahdian and S. Saic. Using Noise Inconsistencies for Blind Image Forensics. Image and Vision Computing, 2009.

[10] K. Francis, S. Gholap, and P. K. Bora, "Illuminant colour based image forensics using mismatch in human skin highlights," *20th Natl. Conf. Commun. NCC 2014, 2014*

[11] S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments," *Ieee Transactions on Information Forensics and Security*, vol. 8, pp. 1355-1370, Aug 2013.

[12] J. Wang, G. Liu, Z. Zhang, Y. Dai, and Z. Wang, "Fast and robust forensics for image region-duplication forgery," *Acta Automatica Sinica*, vol. 35, pp. 1488-1495, 2009.

[13] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in *in Proceedings of Digital Forensic Research Workshop*, 2003.

[14] Sokolova, M., N. Japkowicz, Beyond Accuracy, F-Score and ROC: A Family of Discriminant Measures for Perfor- mance Evaluation, Advances in Arti_cial Intelligence, 4304, 1015-1021 (2006).

[15] Jaberi, M., Bebis, G., Hussain, M., Muhammad, G., Ac-Curate and robust localization of duplicated region in copy-Move image forgery, Machine Vision and Applications, 25(2), 451-475 (2014).

Author Profile

Mohanad F. Jwaid Al-Husseinawi was born in Baghdad, Iraq1988. He received his Bachelors in Engineering of Computer Techniques from Al-Mammon University Collage, Baghdad, Iraq 2014. He took his Masters in Engineering of Information Technology from Maharashtra Institute of Technology (MIT), Pune University, Pune, India 2017. His areas of interest include Image Processing, communications.

Husam K. Salih Jubori was born in Baghdad, Iraq1989. He received his Bachelors in Engineering of Computer Techniques from Al-Mammon University Collage, Baghdad, Iraq 2014. He took his Masters in Engineering of Information Technology from Maharashtra Institute of Technology (MIT), Pune University, Pune, India 2017. His areas of interest include Image Processing, Artificial Intelligence.

Saif A. Salim was born in Baghdad, Iraq1992. He received his Bachelors in Engineering of Computer Techniques from Al-Mammon University Collage, Baghdad, Iraq 2014. He took his Masters in Computer Engineering from DR.DY Patil Institute of Technology, Pune University, Pune, India 2017. His areas of interest include Big Data, Image processing.

Ahmed Q. Mohammed was born in Baghdad, Iraq1989. He received his Bachelors in Engineering of Computer Techniques from Al-Mammon University Collage, Baghdad, Iraq 2013. He took his Masters in Computer Engineering from DR.DY Patil Institute of Technology, Pune University, Pune, India 2017. His areas of interest include Big Data, Image processing.