Pertanika J. Sci. & Technol. 25 (2): 507 - 518 (2017)

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

An Approach for Identification of Copy-Move Image Forgery based on Projection Profiling

Mohd Dilshad Ansari[1]*, Satya Prakash Ghrera[1] and Mohd Wajid[2 #]

[1]*Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, Solan 1732 34, India*

[2]*Deparment of Electronics and Engineering, Jaypee University of Information Technology, Waknaghat, Solan 1732 34, India*

ABSTRACT

An image forgery is a common problem which causes the negative impact on society. In the earlier period it did not affect the general public because the sophisticated image processing software and editing tools were not easily available. Thus, the rapid growth of the image processing software makes this task pretty easy. If it is done with care then it is very difficult for humans to recognize visually whether the image is original or forged. Therefore, the authenticity of an image is a necessity of today's digital era. The copy-move image forgery is the most common type of image forgery in which an area or object is copied and pasted at some other places within the same image in order to hide some important features of the image. In this paper, we have proposed copy-move image forgery detection technique based on the image projection profiling. First, we convert the input image into binary image. The horizontal and vertical projection profiles, which are used in estimating the rectangular regions of copy-move image forgery, are then calculated. The experimental result shows that the proposed approach is able to detect copy-move region successfully and significant improvements have been suggested in computational time compared to other reported algorithms. The performance of proposed approach is demonstrated on various forged images.

Keywords: Copy-move forgery detection, image forgery, image projection profiling, tampering

INTRODUCTION

If image forgery is done with care without leaving any traces, then it is very difficult for a human visionary system to recognise whether the digital image is original or forged. The fast growth of the digital image processing software and internet makes this task pretty easy where anybody can easily

Article history:
Received: 29 April 2016
Accepted: 30 August 2016

E-mail addresses:
m.dilshadcse@gmail.com (Mohd Dilshad Ansari),
sp.ghrera@juit.ac.in (Satya Prakash Ghrera),
wajidiitd@ieee.org (Mohd Wajid)
*Corresponding Author

[#] Author's Current Affiliation:
Department of Electronics Engineering,
Zakin Husain College of Engineering and Technology,
Aligarh Muslim University, 202002 Aligarh, India

ISSN: 0128-7680

doctored digital image with the help of these available tools (Ansari & Ghrera, 2014). This tendency indicates serious vulnerabilities and decreases the trustworthiness of the digital images. Therefore, new techniques should be developed to authenticate the integrity and the genuineness of digital images. This is extremely important in today's digital era, especially taking into consideration that these images can be presented as evidences in a court of law, as news items, as parts of a medical records, as financial documents, or can be used in some other significant places. Therefore, digital image forgery detection is critical.

The most common type of image forgery is copy-move image forgery that is frequently used for doctoring digital image. In this type of image forgery, an object or an area of an image is copied and pasted onto another part of the same image to cover some important features of the image. The task of detecing image forgery becomes more complicated because the copied area will have similar characteristics of the image such as noise component, color palette, texture, etc. This indicates that detection approaches that search for copy-move forgery regions using inconsistencies in statistical measures will fail. There are a number of approaches that give solutions for copy-move image forgery detection. Each of these approaches gives a solution under a set of circumstances or assumptions; these techniques will not work if these assumptions are not realised (Fridrich et al., 2003; Huang et al., 2008; Lin et al., 2011).

Digital image forgery detection techniques are categorised into two approaches: active and passive. In the active approach, the digital image requires preprocessing of image such as watermark embedding or signature generation, which limits their application in practice (Ansari & Ghrera, 2014; Farid 2009). Unlike the watermark and signature-based methods, the passive techniques do not need any digital signature to be generated or to embed any watermark. The passive or blind image forgery detection techniques roughly can be divided into five categories as shown in Figure 1. These are (a) Pixel-based techniques that detects statistical anomalies introduced at the pixel level, (b) the format-based techniques leverage the statistical correlations introduced by a specific lossy compression scheme, (c) camera-based techniques exploit artifacts introduced by the camera lens, sensor, or on-chip post-processing, (d) the physical environment-based techniques explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light, and the camera, and (e) the geometry-based techniques make measurements of objects in the world and their positions relative to the camera (Ansari & Ghrera, 2014; Farid 2009).

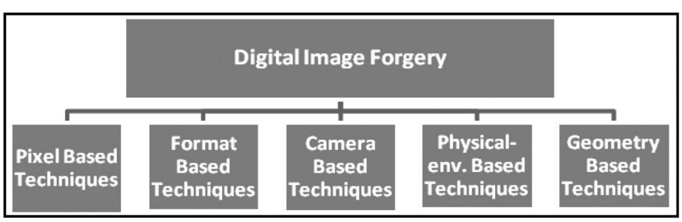


Figure 1. Types of image forgery techniques

The projection profiling of an image contains significant characteristics of an image, which can be used in detecting and estimating many features of an image. In addition to that, it is less computational compared to other image characterising techniques. The image profiling has been used in recognising Braille character pattern (Wajid et al., 2011; Wajid & Kumar 2014). In this paper, we have also used image projection profiling, which helps in detecting copy-move forgery regions in an image.

The remaining part of the paper is organised as follows. In the Background section, we discuss the various copy-move image forgery detection techniques. In the Proposed Method and Algorithm section, we have proposed an algorithm for detecting copy-move image forgery. In the Result and Discussion section, the results are discussed. Finally, the Conclusion section provides the conclusion of this paper.

BACKGROUND

In the direct method for detecting forgeries the image is divided into small overlapping blocks and then all the blocks are compared with one another. If two blocks are found to be similar, then these blocks represent potential forgeries. Suppose the image contains n×n pixels, the block size b×b pixels and the blocks are compared pixel by pixel, then there are $((n-b+1) \times (n-b)/2) \times b^2$ comparisons.

If n = 256 and b = 16, then there are 7.4 million comparisons. That is why these direct approaches are too slow for detecting forgeries from the digital images. In order to make the computation fast and overcome direct method for detecting forgeries, Fridrich et al. (2003) have proposed an effective block-based method, in which the image blocks are represented by quantized Discrete Cosine Transform (DCT) coefficients and a lexicographic sort is applied to detect the similar blocks. Popescu and Farid (2004) have developed a similar approach, applied the Principal Component Analysis (PCA) to yield a reduced dimension representation and computed eigenvalues, eigenvectors of each block for detecting copy-move regions. Ansari and Ghrera (In Press) have proposed noble method for extracting texture feature from the input image, further extracted feature vector can be used to detect copy-move forgery detection. Li et al. (2007) have presented a sorted neighborhood method based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). In this approach, first DWT is applied to the input image and then SVD is used on low-frequency components to reduce their dimensions. Singular value vectors are then lexicographically sorted, similar blocks will be nearby in the sorted list and forgery region is detected. The DWT and SVD methods suffer from the disadvantage that the computation of SVD takes lot of time and it is computationally complex. Bayram et al. (2009) used a scale and rotation invariant Fourier Mellin Transform (FMT) and the notion of bloom filters to detect copy-move image forgery. Their approach is computationally proficient and able to detect forgery in highly compressed images.

Small amounts of work have been reported on copy-move image forgery detection based on "*key point matching*". Huang et al. (2008) have proposed Scale Invariant Feature Transform (SIFT) descriptors for detecting copy-move forgery detection. After extracting the descriptors of different regions, they match them with each other to find possible forgery region in the images. Lin et al. (2011) proposed an integrated method for copy-move forgery and splicing detection. First, image is converted into the YCbCr color space. For splice detection, the image is divided into sub-blocks and DCT is used for feature extraction, SURF is used for copy-move detection.

Most of the above methods suffer from false positives and are not computationally efficient (Fridrich et al., 2003; Kang et al., 2010; Wang et al., 2011). Therefore, the goal of the image forensics is to provide accurate results with less computational time. We have proposed an efficient algorithm for detecting copy-move region successfully with a tool, i.e. projection profiling, which suggests a new improvement in computational time, as shown in Table 1.

PROPOSED METHOD AND ALGORITHM

The algorithm of the proposed approach is given below.

1. Convert an Image $\mathbf{I}$ (color/gray) of order (M, N) into binary image, $\mathbf{J}$.
2. Let $h(j)$ and $v(i)$ be the horizontal and vertical projection profile of $\mathbf{J}$ respectively,they are defined as:

$$h(j) = \sum_{i=1}^{M} \boldsymbol{J}(i, j)$$

and,

$$v(i) = \sum_{j=1}^{N} \boldsymbol{J}(i, j).$$

3. $r(n) = \frac{1}{L}\sum_{l=0}^{L-1} \boldsymbol{\delta}(n - l)$. Consider a moving average filter of order L with impulse response assume, $L \ll min(M, N)$
4. Pass the horizontal and vertical projection profile h and v through this filter and let $h^{'}$ and $v^{'}$ be the outputs of this filter as given below,

$$h^{'}(j) = \sum_{k=1}^{L} r(k)h(j - k)$$

and,

$$v^{'}(i) = \sum_{k=1}^{L} r(k)v(i - k)$$

5. Find the means of these outputs of the filter

$$m_h = \frac{1}{N}\sum_{j=1}^{N} h'(j)$$

$$m_v = \frac{1}{M}\sum_{i=1}^{M} v^{'}(i)$$

6. Search for the corner indexes of the rectangular regions of the copy-move part.
   Let, $h_s = h_e = v_s = v_e = \phi$, where ϕ is a null set.

$for\ j \rightarrow 1{:}N$

$if\ h'(j) < m_h$

$h'(j) = 1$

$else$

$h'(j) = 0$

$h''(j) = h'(j) - h'(j-1)$

$if h''(j) = 1$

$hs = [hs, j]$

$if h''(j) = -1$

$he = [he, j]$

end

$for\ i \rightarrow 1{:}M$

$if\ v'(i) < m_v$

$v'(i) = 1$

$else$

$v'(i) = 0$

$v''(i) = v'(i) - v'(i-1)$

$if v''(i) = 1$

$vs = [vs, i]$

$if v''(i) = -1$

$ve = [ve, i]$

end

7. Identify the rectangular regions of the copy-move part of the image **I**

$$\boldsymbol{R_1} = \mathbf{I}(hs(1,1){:}\ he(1,1), vs(1,1){:}\ ve(1,1))$$

and,

$$\boldsymbol{R_2} = \mathbf{I}(hs(1,2){:}\ he(1,2), vs(1,2){:}\ ve(1,2))$$

Where, $\boldsymbol{R_1}$ and $\boldsymbol{R_2}$ are the matched regions.

RESULT AND DISCUSSION

The experimental results were carried out on MATLAB, 4GB RAM and core i3 processor. To check the robustness and feasibility of proposed algorithm, we have tested algorithm on more than 20 forged images with various image sizes, 128×128, 256×256 and 512×512, etc.

Figure 2(a) shows original image which is forged by copy-move techniques shown in Figure 2(b), where an object is copied and pasted on the same image at some other location. The forge image is converted into binary image; thereafter the horizontal and vertical projection profile of image is taken, shown in Figures 3 and 4, respectively. Further, moving average filter has been applied on these projection profiles, which has smoothen these curves (also shown in Figure 3 and Figure 4). From the filtered horizontal projection profile, the x-coordinate of the corners of the rectangle boxes have been calculated, as given in algorithm. Similarly, the y-coordinate has been calculated using filtered vertical projection profile. The algorithm is also evaluated on other forged images as shown in Figures 5-16.The proposed technique is robust even though multiple objects are available in the image, which is based on the repetitions of the valleys in the projection profile. From the projection profile, we can identify the number of copy-move objects in the forged image. If another distinct object is available in the image, it can contribute to a valley in the projection profile but will not match with any other valley in the same projection profile. However, the proposed technique is limited to the case when the object is having contrast to the background of the image. The computational time efficiency is compared with the existing method shown in Table 1. It has been shown that computation time is relatively less for the proposed method for different sizes of images. For the proposed algorithm, there is a tremendous improvement in the computation time for the bigger image sizes.

(a) (b) (c)

Figure 2. (a) Original image; (b) Forged image; (c) Detected region of copy-move forgery

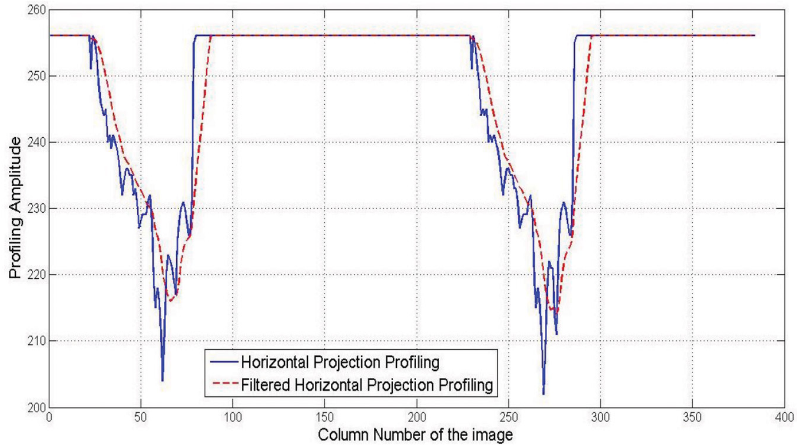


Figure 3. Horizontal projection profile and filtered horizontal projection profile for the image shown in Figure 2(b)

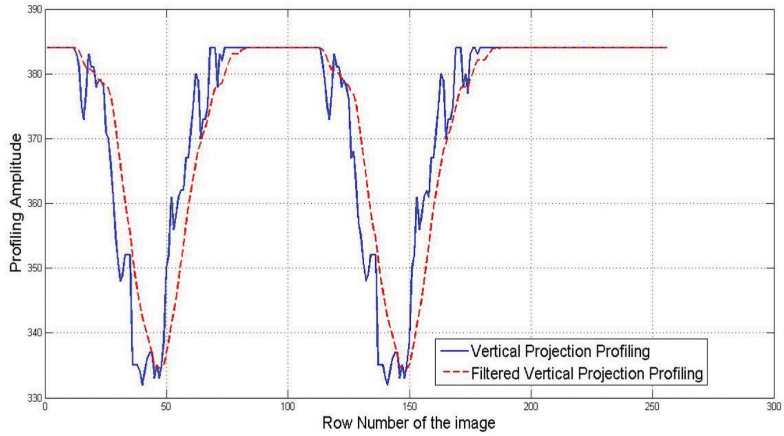
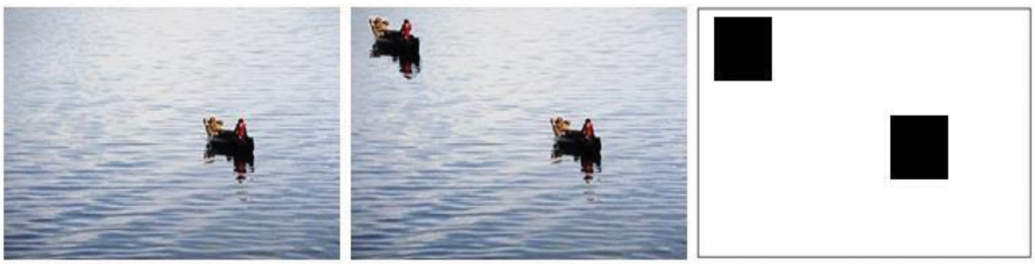


Figure 4. Vertical projection profile and filtered vertical projection profile for the image shown in Figure 2(b)



(a) (b) (c)

Figure 5. (a) Original image; (b) Forged image; and (c) Detected region of copy-move forgery

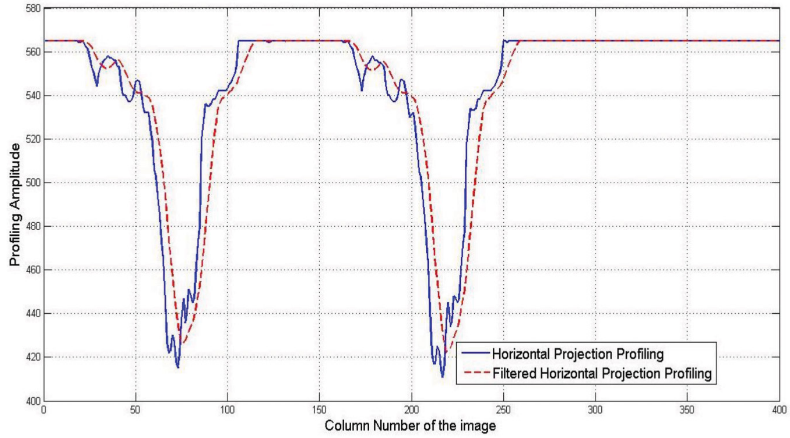


Figure 6. Horizontal projection profile and filtered horizontal projection profile for the image shown in Figure 5(b)

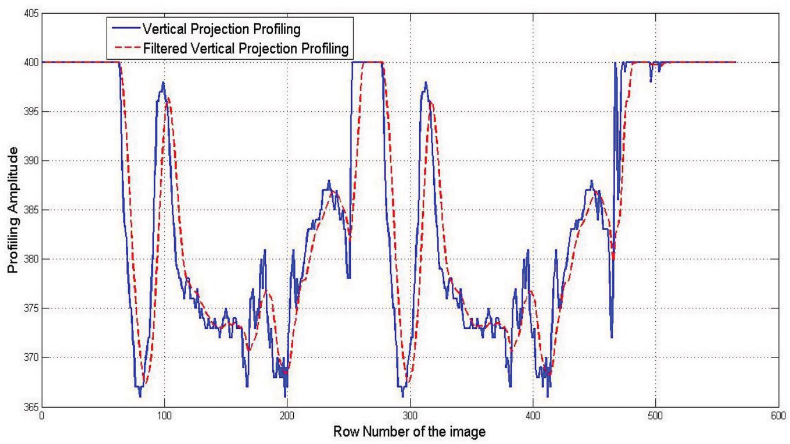


Figure 7. Vertical projection profile and filtered vertical projection profile for the image shown in Figure 5(b)

(a) (b) (c)

Figure 8. (a) Original image; (b) Forged image; and (c) Detected region of copy-move forgery

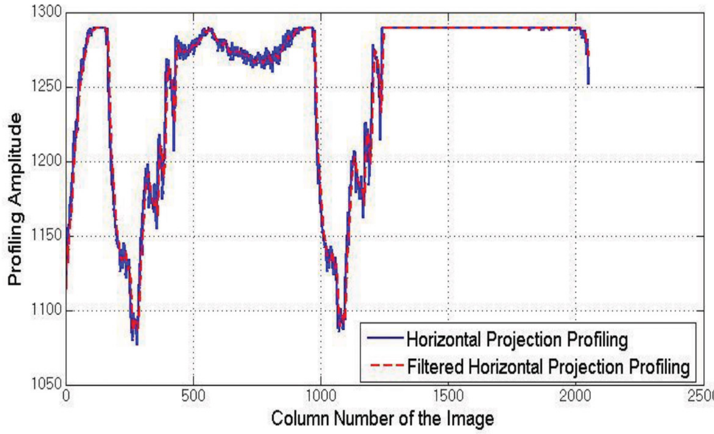


Figure 9. Horizontal projection profile and filtered horizontal projection profile for the image shown in Figure 8(b)

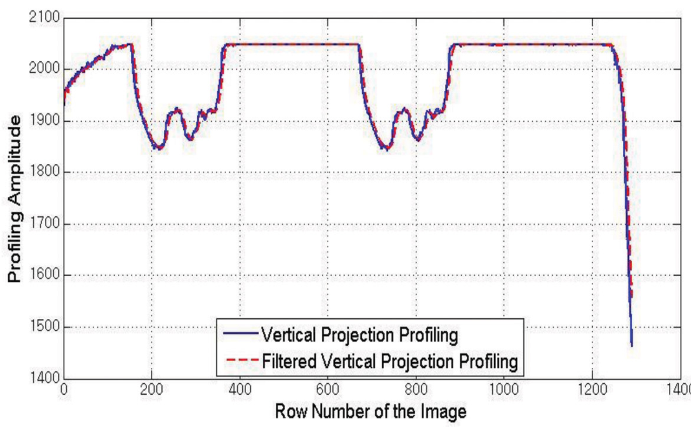


Figure 10. Vertical projection profile and filtered projection profile for the image shown in Figure 8(b)

(a) (b) (c)

Figure 11. (a) Original image; (b) Forged image; and (c) Detected region of copy-move forgery

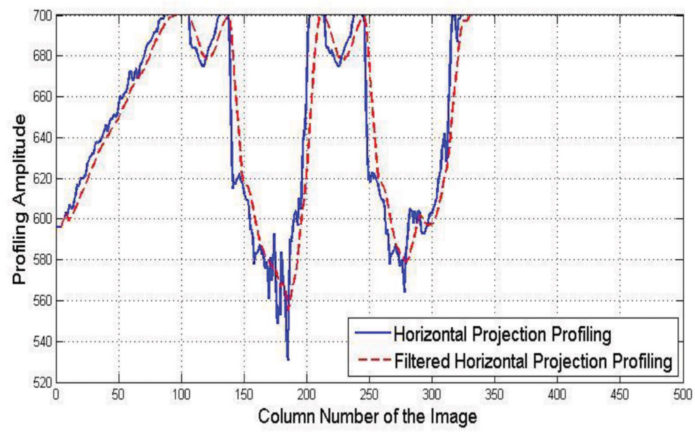


Figure 12. Horizontal projection profile and filtered horizontal projection profile for the image shown in Figure 11(b)

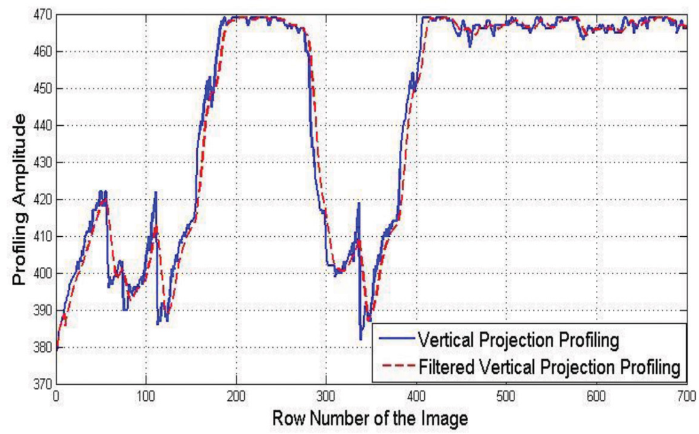


Figure 13. Vertical projection profile and filtered vertical projection profile for the image shown in Figure 11(b)

(a) (b) (c)

Figure 14. (a) Original image; (b) Forged image; and (c) Detected region of copy-move forgery

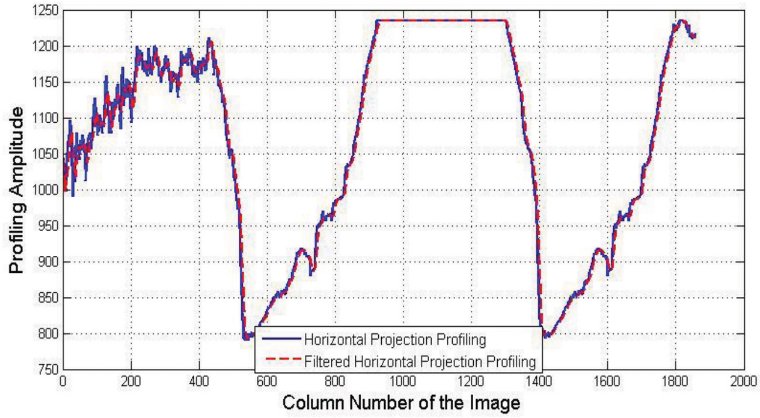


Figure 15. Horizontal projection profile and filtered horizontal projection profile for the image shown in Figure 14(b)

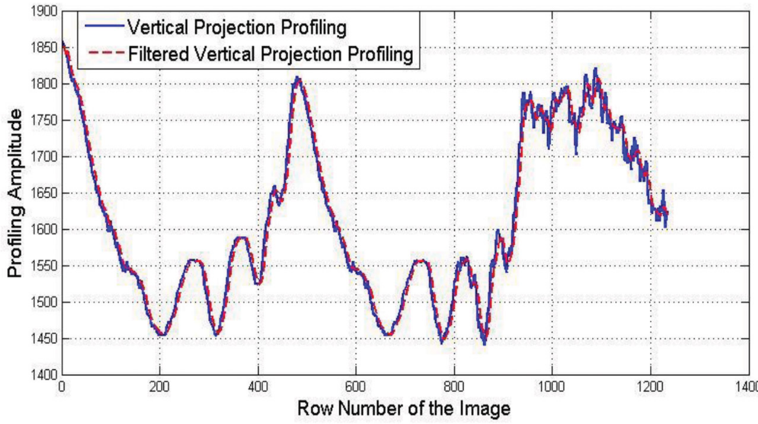


Figure 16. Vertical projection profile and filtered vertical projection profile for the image shown in Figure 14(b)

Table 1
Copy-move forgery detection execution time in seconds

Image Name	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6	Image 7
Image Size	128×128	256×256	384×384	424×424	512×512	656×656	832×832
Xiaofeng Wang et al.	4.96	39.70	171.09	239.48	478.109	1259.35	1308.25
Proposed Method	3.29	4.27	4.81	5.33	5.69	6.12	6.84

CONCLUSION

We have proposed a new method for image forensics based on projection profiling. As the block-based copy-move forgery detection methods are computationally intensive any improvement in execution time will help in checking forgery from the given image. The proposed method successfully addresses this issue and is noticeably faster than the existing methods. To check the robustness of our proposed approach it has been performed on various forgery images. The results show that the proposed approach is able to detect copy-move region effectively and new improvements have been suggested in computational time shown in Table 1. In the future, we can improve the copy-move forgery detection approach by applying various attacks such as rotation, scaling, added Gaussian noise, JPEG Compression, etc.

REFERENCES

Ansari, M. D., Ghrera, S. P., & Tyagi, V. (2014). Pixel-Based Image Forgery Detection: A Review. *IETE Journal of Education*, *55*(1), 40-46.

Ansari, M. D., Ghrera, S. P. (n.d.). Intuitionistic fuzzy local binary pattern for features extraction. *International Journal of Information and Communication Technology.* In Press

Bayram, S., Sencar, H. T., & Memon, N. (2009, April). An efficient and robust method for detecting copy-move forgery. In *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on* (pp. 1053-1056). IEEE.

Fridrich, A. J., Soukal, B. D., & Lukáš, A. J. (2003). Detection of copy-move forgery in digital images. In *in Proceedings of Digital Forensic Research Workshop*.

Farid, H. (2009). Image forgery detection. *Signal Processing Magazine, IEEE*, *26*(2), 16-25.

Huang, H., Guo, W., & Zhang, Y. (2008, December). Detection of copy-move forgery in digital images using SIFT algorithm. In *Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on* (Vol. 2, pp. 272-276). IEEE.

Kang, Li., & Cheng, X. P. (2010). Copy-move forgery detection in digital image. In *Image and Signal Processing (CISP), 2010 3rd International Congress on* (pp. 2419-21). IEEE.

Li, G., Wu, Q., Tu, D., & Sun, S. (2007, July). A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. In *Multimedia and Expo, 2007 IEEE International Conference on*(pp. 1750-1753). IEEE.

Lin, S. D., & Wu, T. (2011, October). An integrated technique for splicing and copy-move forgery image detection. In *Image and Signal Processing (CISP), 2011 4th International Congress on* (Vol. 2, pp. 1086-1090). IEEE.

Popescu, A. C., & Farid, H. (2004). *Exposing digital forgeries by detecting duplicated image region* [Technical Report 2004-515]. Hanover, Department of Computer Science, Dartmouth College, USA.

Wajid, M., Abdullah, M. W., & Farooq, O. (2011, November). Imprinted Braille-character pattern recognition using image processing techniques. In *Image Information Processing (ICIIP), 2011 International Conference on* (pp. 1-5). IEEE.

Wajid, M., & Kumar, V. (2014). E-Braille Documents: Novel Method For Error Free Generation. *Image Processing and Communications*, *19*(4), 21-26.

Wang, X., Zhang, X., Li, Z., & Wang, S. (2011, November). A DWT-DCT based passive forensics method for copy-move attacks. In *2011 Third International Conference on Multimedia Information Networking and Security* (pp. 304-308). IEEE.