International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 22 (2017) pp. 11855-11861

Literature Review: Detection of Image Splicing Forgery

Araz Rajab Abrahim[1], Mohd Shafry Mohd Rahim[1,2] and Ghazali bin Sulong[3]

[1] Faculty of Computing, Universiti Teknologi Malaysia, Skudai, 81310, Johor Bahru, Malaysia.
[2] IRDA Digital Media Center, Universiti Teknologi Malaysia (UTM), Skudai, 81310, Johor Bahru, Malaysia.
[3]School Informatics and Applied Mathematics, Universiti Malaysia Terengganu (UMT), 21030 Kuala Terengganu, Malaysia.

[1]Orcid: 0000-0002-7259-2178

Abstract

Digital splicing technology has become an influencing factor when it comes to the technological development of digital photo manipulation because of remarkable technology development in this area. The most popular users of digital splicing are those businesses involved in newspaper and magazine publication, companies that require authenticity verification of photographs that will be used in their publications. What was once aa big pre-publication challenge for these companies due to the digital forensics involved in the digital image processing method, can now be ratified within a few keystrokes. This review aims to introduce the reader to the various types of digital image splicing forgeries in relation to the most current trend of passive techniques used to ratify the authenticity of the images prior to publication.

Keywords: Digital image forensics, image forgery detection, Image authentication, , Image Splicing, Passive techniques.

INTRODUCTION

Increased technological developments have enhanced the ease attached to digital image manipulation, which has influenced the level of concern attached to the image splicing process. Poor existence and adoption of image verification processes has led to decreased viability attached to automated content through lack of the necessary and appropriate verification systems. Additionally, the development of automated algorithms influence the possible level of manipulation, which delimits the level of human inspection leading to increased manipulation of images due to lack of the necessary verification systems [1].

In addition to images many algorithms applied on text for recognize scripts which is done by the segmentation where is play a vital role in script recognition process[2] A practical recorded scenario was exemplified early in 1840s. Hippolyta Bayard was the first person to tamper with an image through forgery. He produced a false image in which he appeared committing suicide, just as illustrated in figure 1 below. This trick was only a response to Louis Daguerre, originator of the Daguerreotype, getting a copyright for a photographic development prior any efforts by Bayard, a great deal to Bayard's aggravation [2].

Figure 1: First photographic forger [2]

CLASSIFICATION OF IMAGE FORGERY DETECTION TECHNIQUES

Forgery identification aims at verifying the image's authenticity [3]. In order to attain excellent authenticity of images, a wide range of approaches have been proposed. This paper classifies these approaches into two forms: Passive authentication and active authentication. This categorization is founded on the verity regarding the availability of the original image, if it's available or not, forgery is classified being hierarchical as portrayed in figure 2.

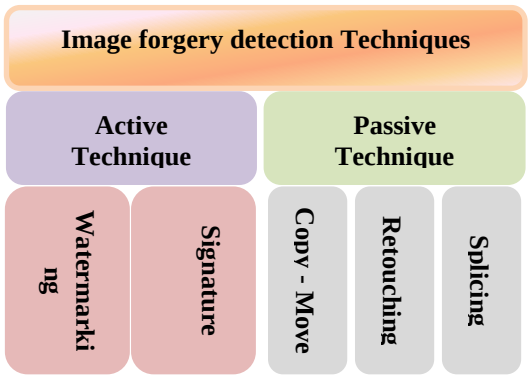


Figure 2: Authentication Techniques of Image

Active Techniques

In the age of fake news, not only verbal reports can be falsified for presentation to the public, but images of events, incidents, and people as well. These digital representations of the real person are used along-side the fake news in order to give the report a sense of authenticity. Simply put, a fake image is something that is spliced together using active techniques. Several of these active techniques are based upon initial passive falsification recognition based upon ideologies set forth by the active techniques. ([4], [2]).

This practice, though practiced actively in the past, had limited applications types:

Watermark – A digital watermark is integrated into an image being captured, supported by an integrity authentication on the recipient side.

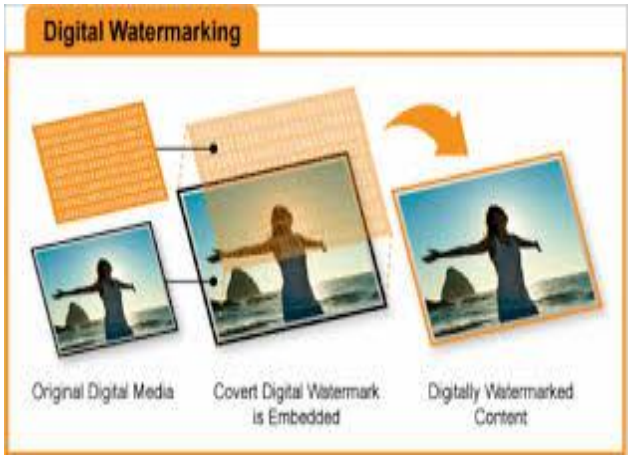


Figure 3: The conversion process from original media to digital watermarked content.

Signature – A camera's image will be extracted of its distinct aspects and then data encoded using a signature.

Passive Techniques

This technique is equally referred to as image forensics. Unlike active approaches, blind (passive) approaches utilized in detecting counterfeit images utilize the lead of left traces during steps dispensation in diverse stages while acquiring and storing digitally acquired images [5].

Such traces can be regarded as the image source's fingerprint. Passive techniques operate without the presence of protecting criteria. They do not utilize any pre-image informational allocation slotted into digital image. Additionally, these techniques employ simply the image function and the condition that certain image changes could be realized in case the image had been tampered with. Their operation entails an analysis of the image's binary data for the purposes of discovering any traces of forgery activity [6].

Passive authentication is further divided into:

1- Forgery dependent Approach - Forgery dependent identification approaches are designed to identify some specific type of forgeries for instance splicing and copy-move which depend on the forgery type enacted on an image.

2- forgery independent approach - forgery independent approaches detect interferences which are not dependent on the type of forgery, but founded on the artifact traces left behind during the re-sampling procedure as well as lighting errors [7].

Copy-move Forgery Detection

This is the highly known and common technique of altering an image since of the ease and simplicity of operation [8].

It entails copying some parts of an original's image and pasting them to another section of a novel image. Because the merged part belongs to an identical image, then the dynamic color and range hold their compatibility mode with the remaining part of the image [9]. Figure 4 exhibit a perfect exemplar of copy-move forgery.

Tampered Original

Figure 4: Copy- move Forgery. [10]

Image Retouching

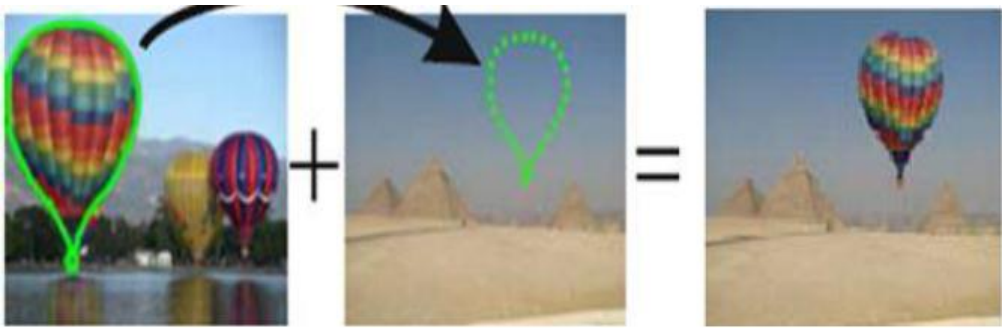
This tool is an additional criterion engaged in image forgery and it is extensively employed for aesthetic and commercial purposes. Retouching procedures are conducted particularly to reduce or facilitate the features and quality of the image. Equally, retouching technique is conducted to generate a more convincing compound of the merged images which

may need resizing, rotation, or stretching one of the merged images. The figure 5 exemplifies this technique. The engaged piece of photography was issued by Iranian military.

Figure 5: Re-sampled image: Launching of Missile weapon by Iranian military

Image Splicing

Image splicing requires the altering of one image using a merging or compositional approach to editing. The forged image normally shows a conflicting background which is the result of trying to merge differencing boundaries and borders of separate pictures. The image below (Figure 6) shows the steps involved in creating a spliced image using a source image which will then be copy-pasted into a target image.



a. Source image b. Target image c. Composite image

Figure 6: Image splicing equation

These types of image forgeries can be completed convincingly by even an amateur photographer using commercially available photo editing software. The image just needs to be manipulated by lifting a part of the source image (a) onto the target image (b). [11] These types of splicing can be done with the least of difficulties even by beginners in the profession.

It is important to understand how image splicing is done because this process seems to be the procedure of choice for most image forgers. These types of alterations do now show visual signs of tampering as an actual print photograph would. By creating and image from a number of images, the photograph becomes an almost authentic version that is usable for the purpose of the report or article.

In figure 7, an example of image splicing and its required steps to complete the process is featured. [11]

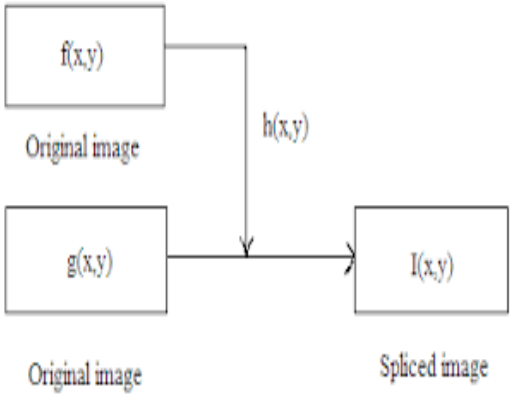


Figure.7: The steps of image splicing, f(x,y) and g(x,y) are original images, h(x,y) these are a part of f(x,y) which is inserted into g(x,y) that then generates a spliced image I(x,y). Perhaps f(x,y) and g(x,y) are the same image.

General framework for image forgery system

IFDS (Image Forgery Detection System) is a type of PRS (Pattern Recognition System) whose purpose is to allocate one of pre-ideal categories to an unidentified input pattern. In such image patterns in the FDS, the classification entails forged and authentic images. A distinctive IFDS entails 5 major steps, as shown in the figure 8.

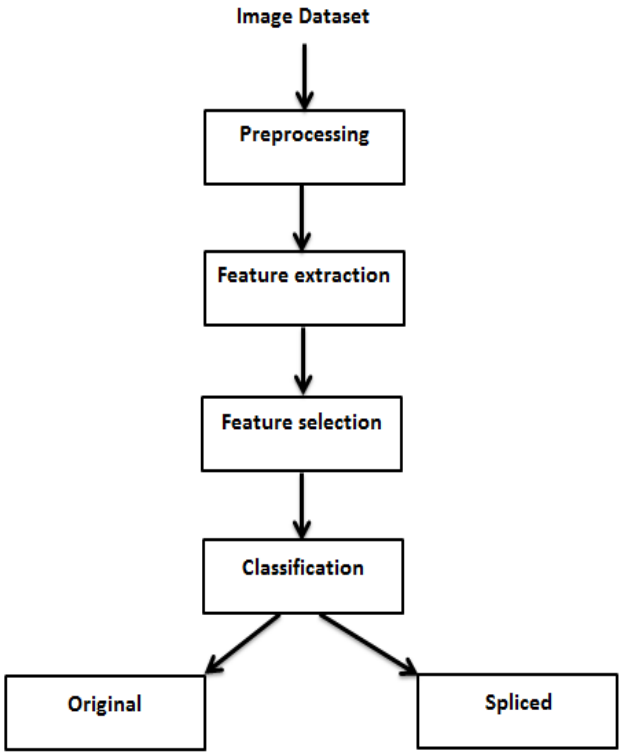


Figure 8: Flowchart of the main components of IFDS.

Image preprocessing is the first step of process entails the application of image enhancement mechanisms with the intent of either isolating interest patterns or reduction of noise from the background.

Feature extraction process involves searching for a novel method of data (image) illustration in view of aspects. The principal intent is the extraction of discriminant aspects that portray the image adequately. Prevention of redundancy and minimizing the data dimensionality are two prerequisites for excellent features. Diverse techniques are employed in the detection of image forgery as well as features extraction ([12], [13] and [3]).

Next process is feature selection; this entails the technique of selecting a detachment of the extracted aspects to minimize the dimensions of the characteristics as well as the time intricacy. This can be achieved through eradication of any unimportant and redundant features. Several and varied techniques of features selection have been stipulated, for instance SFS (Sequential forward selection) and CFS (Correlation based Feature Selection) approaches [14].

Classification process entails the criterion of getting unknown data sample assigned to one of the predefined categories. Data (with identified classes) is engaged in modeling a classifier. The process entails two stages: training stage and testing stage shown in figure 9.

Categorization can be in form of multiclass or tow-class with respect to total classes in the data. There are several techniques employed in the classification process, with some of the famous schemes being Neural Network (NN), Nearest Distance Classifier (NDC), and Support Vector Machines (SVM) ([15], [16], and [17]).

In IFD, several researchers and scholars engaged SVM algorithm [3]. The subsequent section offers a concise analysis of this type of algorithm.

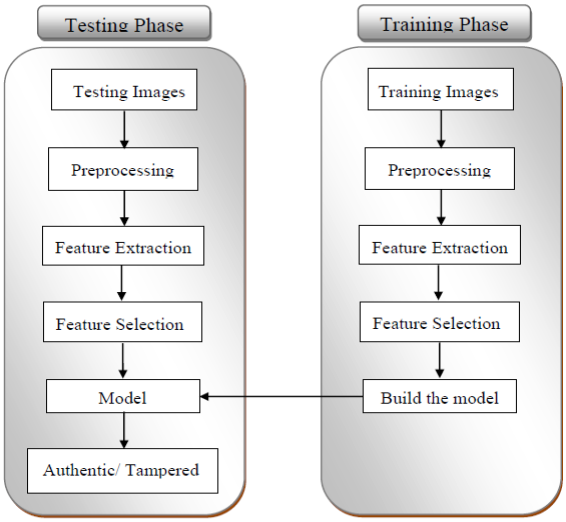


Figure 9: The training and testing phases of the classification.

LITERATURE SURVEY

This detailed literature survey has been completed to provide a detailed analysis of image splicing forgery techniques. Techniques with regards to detecting image splicing forgeries are presented in this review paper.

It would be possible to reveal a spliced image if one checks for camera characteristics consistency in various unnoticeable parts of the image. The fully automatic spliced image would have differences in distinct areas of the photographs. By estimating the camera response function (CRF) using geometric invariants from locally planar irradiance points (LPIPs), the boundary segment of the two

areas may be discovered to be either authentic or spliced. [18]. The data from the images can be analyzed using SVM-based classifiers that result in 70% precision and 70% recall.

The human visual model suggested by [19] may also be used to identify fake imaged using automatic detection framework using visual saliency and fixation on a forensic basis. While this is a convenient method for proving spliced images, there is a learning curve required in order to accurately accomplish this task.

There is a suggestion [20] that tampered images can be proved using modeling edge information. The Chroma of the image near the edge of the photograph is considered a finite-state Markov chain the requires the extraction of low dimensional feature vectors emanating from stationary distribution that can be used for tampering detection. A Support Vector machined is utilized to consider the usability and effectiveness of the algorithm proposed.

The proposed algorithm based on Markov in Quaternion discrete cosine transform (QDCT) is used for image splicing detection [21]. The SVM is used to classify the images in accordance with the proposed algorithm which makes use of color information within the images, thus resulting in a high classification accuracy.

The Barrel also Pincushion based on Polaroid parameter of specific lens spiral twisting may also be used to prove picture grafting [22]. This paper will suggest that indifferent system is a useful tool in determining if an image is copy – pasted through quantitative measurement of lens spiral twisting in various areas of the photo via line-based alignment. The test has shown that a number of customer level advanced cameras can claim lens spiral twisting based upon the applicable zoom level. This could then be misinterpreted as a spliced picture due to the Picture Joining that occurs on a zoom level.

One may also consider class dependences based upon 3 successive classes and transition probability in order to determine image splicing [23]. The transition probabilities can be determined using the progression of the current class to the next 2 classes while looking for discriminative features. Conditional co-occurrence probabilities are analyzed as a group (CCPM) with a matrix fed into the SVM for proper classification. Depending of the higher order statistical features that contain discriminative information on the photo, a possible high dimensionality could lead to a computational complexity along with an over-fitting for the modern supervised classifier. So dimensionality reduction (PCA) is strongly suggested for use in this instance.

Some experts suggest that motion blur estimation based on image gradients can also be used to detect possible irregularities in an image based upon the possible spliced region [24]. The motion blur can be measured based upon inconsistent region segmentation of the images that contain a small amount of blur.

Suggestions [25] that the detection be done by determining specific artifact based on Markov features which were acquired using DCT domain and DWT with the best features selected by SVM-RFE can be used to compute LBP for each pixel. The resulting LBPed image and partitioned LBPed imaged will then be based on Slantlet transform using Standard Deviation to create the feature vector based upon SVM classification.

[26] are the pioneers of the multi-resolution Weber law descriptors (WLD) based image forgery detection method. Since there are countless digital image processing techniques and software tools which edit images without leaving an obvious digital footprint, the authentication of these images is important to the accurate education and information of people. Using the multi-resolution WLD to extract chrominance components, a support vector machine can help determine the forgery of an image using an image database containing image forgery information.

There is a suggestion from [27] that advanced picture experiences extreme danger because any image can now be altered to suit the requirements of the user without having to totally abandon the use of a photo. By using double example (LBP) along with discrete cosine the senior change (DCT) may also be used. The idea is that the chrominance part of the picture information is isolated under covering squares. Then the LBP can be determined per block and converted under recurrence Web-domain utilizing 2D DCT. The standard deviations are predicted in terms of recurring coefficients in every last square. The SVM machine can be used to classify once again. Test benchmarks will show that the identification exactness will be increased to 97%, the best exactness possible.

Partial Blur Type Consistency as suggested by [28] may also be used using block – based image partitioning by extracting the local blur type from estimated local blur kernels. These image blocks are called out-of-focus and generate invariant types of blur regions. Fine splicing localization is used to increase region Fine splicing localization is used to increase region boundary precision to help trace for any inconsistencies in the image based on splicing localization. Experiments have shown that this method is an applicable testing technique

Table 1: Comparison table

Authors	Year	Method	Dataset	Detection Accuracy (%)
Hsu and Chang.[18], (2007)	2007	CRF& LPIP	own dataset	Precision-70 Recall 70
Qu, Qiu and Huang.[19] ,(2009)	2009	human visual system (HVS)	Columbia	96.33
Kong and Box. [20],(2010)	2010	modeling the edge image of chroma component as a finite-state Markov chain & extract low dimensional feature vector from its stationary distribution .	Columbia	93.55
Wei, Gulla and Fu.[21], (2010)	2010	QDCT	DVMM	93.42
Chennamma and Rangarajan.[22], (2011)	2011	consistency of lens radial distortion	Columbia	86
Zhao *et al.*. [23], (2011)	2011	conditional co-occurrence probability matrix (CCPM)	Columbia	Markov 86.8 - CCPM 88.5
Kakar, Sudha and Ser. [24], (2011)	2011	spectral analysis of image gradients	own dataset	93.43
He *et al.*. [25], (2012)	2012	Markov features generated, DCT, DWT, feature selection method SVM-RFE	CASIA 2	95.50
Hussain *et al.*. [26], (2013)	2013	multi-resolution Weber law descriptors (WLD) based image forgery detection	CASIA 1	93.33
Alahmadi *et al.*[27], (2013)	2013	LBP, DCT	CASIA 1	97.7
Bahrami and Kot. [28], (2015)	2015	partial blur type inconsistency	Own dataset	96.3

CONCLUSION

These days, anti-social people have taken to using fake images (spliced images) to created scenes that they can misuse in any form they wish. This unscrupulous act has led to the necessity of authenticating images used in all media platforms (e.g. newspapers and magazines). While extensive research on image splicing has been done, there are still a number of challenges that exist in the identification of image manipulations. Even through image splicing can now be determined there are still a number of factors that need to be addressed before an accurate digital image authentication process can be created. These problems include: sourcing the original image to reveal tampering and image resolution issues, and still there are types of images called (shallow depth of field) the review techniques failed to detect these images whether they are authentic or spliced. The literature review presents several methods of image slicing detection and shows hope for a more complex but more accurate future Digital Forensic analysis field.

REFERENCES

[1] Sridevi M, Mala C, Sanyam S.(2012). Comparative study of image forgery and copy-move techniques. Adv Intell Soft Comput,166 AISC(VOL. 1),715–23.

[2] Harouni, M., Rahim, M. S. M., Al-Rodhaan, M., Saba, T., Rehman, A., & Al-Dhelaan, A. (2014). Online Persian/Arabic script classification without contextual information. *The Imaging Science Journal*, *62*(8), 437-448.

[3] Lin C, Chang S.(1998). Generating Robust Digital Signature for Image / Video Authentication. Multimed Secur Work ACM Multimed '98, Bristol, UK.

[4] Birajdar GK, Mankar VH.(2013). Digital image forgery detection using passive techniques: A survey Digit Investig,10(3),226–45.

[5] Name L, Name F, Training O, Training P, Darin C, Training RO, et al.(2014). No Title No Title. Igarss, 2014. 1-5 p.

[6] Zhou Z, Zhang X.(2010). Image splicing detection based on image quality and analysis of variance. In: Education Technology and Computer (ICETC), 2nd International Conference on, p. V4--242.

[7] Farid H.(2009). Exposing digital forgeries from JPEG ghosts. IEEE Trans Inf Forensics Secur, 4(1),154–60.

[8] Redi J a., Taktak W, Dugelay JL.(2011). Digital image forensics: A booklet for beginners. Multimed Tools Appl, 51(1),133–62.

[9] Bruno A, Informatica I.(2010). Copy-Move Forgery Detection via Texture Description. ACM Work Multimed Forensics, Secur Intell Co-located with ACM Multimed, 59–64.

[10] Bravo-Solorio S, Nandi AK.(2011). Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics. Signal Processing, 91(8),1759–70.

[11] Kang X, Wei S.(2008). Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics. 2008 Int Conf Comput Sci Softw Eng, 926–30.

[12] Zhang Z, Zhou Y, Kang J, Ren Y. Study of image splicing detection. Adv Intell Comput Theor Appl With Asp Theor Methodol Issues. 2008;1103–10.

[13] Farid H.(2009). Image forgery detection. IEEE Signal Process Mag, 26(2),16–25.

[14] Mahdian B, Saic S.(2010). A bibliography on blind methods for identifying image forgery. Signal Process Image Commun, 25(6),389–99.

[15] Pevzner P, Waterman M.(2002). Lecture Notes in Bioinformatics. Vol. 51, Systems Biology, 215-229 p.

[16] Xia C, Hsu W, Lee ML. ERkNN.(2005). efficient reverse k-nearest neighbors retrieval with local kNN-distance estimation.14th ACM Int Conf Inf Knowl Manag, 533–40.

[17] Wu J-Y.(2011). MIMO CMAC neural network classifier for solving classification problems. Appl Soft Comput, 11(2), 2326–33.

[18] Cortes C, Vapnik V.(1995). Support-Vector Networks,297, 273–97.

[19] Hsu Y-F, Chang S-F.(2007). Image splicing detection using camera response function consistency and automatic segmentation. In: Multimedia and Expo, IEEE International Conference on, p. 28–31.

[20] Qu Z, Qiu G, Huang J.(2009). Detect digital image splicing with visual cues. In: International workshop on information hiding, p. 247–61.

[21] Kong H, Box PO.(2010). IMAGE TAMPERING DETECTION BASED ON STATIONARY DISTRIBUTION OF MARKOV CHAIN National Laboratory of Pattern Recognition. Institute of Automation , Chinese Academy of Sciences, 2101–4.

[22] Wei W, Gulla JA, Fu Z.(2010). Advanced Intelligent Computing Theories and Applications. Lect Notes Comput Sci (including Subser Lect Notes Artif Intell Lect Notes Bioinformatics) [Internet], 6215(2),380–91.

[23] Chennamma HR, Rangarajan L.(2011). Image Splicing Detection Using Inherent Lens Radial Distortion. Int J Comput Sci Issues [Internet], 7(6),10.

[24] Zhao X, Wang S, Li S, Li J.(2011). Passive detection of image splicing using conditional co-occurrence probability matrix. APSIPA ASC 2011 - Asia-Pacific Signal Inf Process Assoc Annu Summit Conf 2011.

[25] Kakar P, Sudha N, Ser W.(2011). Exposing digital image forgeries by detecting discrepancies in motion blur. IEEE Trans Multimed,13(3), 443–52.

[26] He Z, Lu W, Sun W, Huang J.(2012) Digital image splicing detection based on Markov features in DCT and DWT domain. Pattern Recognit [Internet],45(12),4292–9.

[27] Hussain M, Muhammad G, Saleh SQ, Mirza AM, Bebis G.(2013). Image forgery detection using multi-resolution Weber local descriptors. Eurocon, 1570–7.

[28] Alahmadi AA, Hussain M, Aboalsamh H, Muhammad G, Bebis G.(2013). Splicing image forgery detection based on DCT and Local Binary Pattern. 2013 IEEE Glob Conf Signal Inf Process Glob 2013 - Proc, 253–6.

[29] Bahrami K, Kot AC.(2015). Image splicing localization based on blur type inconsistency. Proc - IEEE Int Symp Circuits Syst, 1042–5.