Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 458 – 465

Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

A Scaling Robust Copy-Paste Tampering Detection for Digital Image Forensics

Anil Dada Warbhe[a*], R. V. Dharaskar[b], V. M. Thakare[c]

[a]*Research Scholar, SGBAU, Amravati 444602, India*
[b]*Former Director, DES (Disha–DIMAT) Group of Institutes, Raipur 492101, India*
[c]*HOD, SBGAU (PG Dept. of Computer Science), Amravati 444602, India*

Abstract

It is crucial in image forensics to prove the authenticity of the digital images. Due to the availability of the using sophisticated image editing software programs, anyone can manipulate the images easily. There are various types of digital image manipulation or tampering possible; like image compositing, splicing, copy-paste, etc. In this paper, we propose a passive scaling robust algorithm for the detection of Copy-Paste tampering. Sometimes the copied region of an image is scaled before pasting to some other location in the image. In such cases, the normal Copy-Paste detection algorithm fails to detect the forgeries. We have implemented and used an improved customized Normalized Cross Correlation for detecting highly correlated areas from the image and the image blocks, thereby detecting the tampered regions from an image. The experimental results demonstrate that the proposed approach can be effectively used to detect copy-paste forgeries accurately and is scaling robust.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: Digital Image Forensics; Image Forgery Detection; Image Tampering; Image Authentication.

1. Introduction

The internet has gifted us cost-effective approach to exchange and trade the data all over the world. Today's world almost entirely relays on internet technologies to communicate, doing businesses and governance. The main features of the technology, like Low cost, speedy access and ease of operation has made human lives easy going. However, all these advantages and the convenience, come at a cost. With increased sophistication of the

* Corresponding author. Tel.: +91-982-355-1869.
*E-mail address:*mtech2008@rediffmail.com

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.059

technologies, Internet crime has also increased tremendously around the world. The Internet has provided a stage for internet criminals to carry out criminal activities and posing a significant threat to Internet users.[1,2,3] These criminal activities are broad and diverse, for example, identity theft, a threat to nation's security, child pornography, copyright infringement is, to name a few. These crimes impose threats to individual safety and privacy. In such scenario, if the criminal get access to the confidential data of a person, such as or photos and videos, etc.; criminal can play with it as he wants, to satisfy his malice intents and poor victim, on the other hand, has to face serious consequences. Image forensics investigators need robust and efficient image authentication procedures to apprehend, detect and take legal action against criminals, involved in such acts.[4]

Digital forensics is a vast domain and covers many disciplines. The authors[5] have presented a complete ontology of digital forensics. The images are the rich source of information and are widespread in the cyberspace. The main concern with these digital images is that they are vulnerable to modifications very easily. Due to the availability of the sophisticated image editing software is on PCs, laptops, and mobile devices, one can easily carry out tampering with it. These attacks on images pose a great danger to the whole community, as one can easily change the meaning of the image by simply carrying out some operations on it. Once it becomes viral on the social networking sites can create havoc. Hence, it is imperative to authenticate the images for their originality. The authenticating the digital images for their content i.e. integrity, the source is the field of Digital Image Forensics (DIF). DIF has gained tremendous importance in last one and half decade among the research community. The fundamental problems digital image forensics techniques attempt to solve is the identification of the source and detecting the integrity of a digital image[6]. Identification of source involves determining the means by which the images are created like camera, scanner, and regenerative algorithm. Similarly, integrity can be confirmed by analyzing the images for its modification.

Digital image forensics can be classified broadly under two heads, as active forensics and passive forensics. Active forensics involves authenticating images by extracting the digital signature or watermark embedded in it. The digital watermarks are inserted into the images by the special cameras at the time of taking pictures. Any tampering operations done on the image can deteriorate the embedded watermark. This detected deterioration can be taken as an indication of the possible image tampering. However, the main limitation of the active forensics is that we need both original and the tampered image to authenticate and confirm tampering. Also, the need for special devices, such as special cameras, for example, makes it a costlier affair. Passive forensics, on the other hand, neither require special devices nor needs to have the original content available to prove tampering of the image. Passive forensics is also termed as blind forensics. It relies on the simple principle that the original natural image always owns some inherent pattern and statistics that are consistent. When some tampering operation occurs on the image, this change in the statistics of the image guarantees image tampering.[7]

Image Forensics or image tampering detection can be classified into different categories, like pixel base, a format based, camera based, etc.[8]. Copy-paste tampering detection comes under pixel based forensic detection tool. It is a most common type of tampering, in which forger copies some region from one place of an image and pastes it at some other location. Though copied and pasted regions in this class are identical; these tampering operations are so smartly done, that it leaves no obvious traces of tampering. It is sometimes easier to detect the pasted regions if it did not undergo any post processing operation. It becomes difficult if the copied part undergoes some sort of transformation such as scaling, rotation or both. In this paper, we introduce a scaling robust copy-paste detection scheme using Normalized cross correlation.

2. Literature Review

Copy-Paste tampering is also called as copy-move forgery. Copy-paste tampering detection can be carried out by two main approaches; either block based or by key-point detection[9,10]. As proposed technique uses the block based approach in this section, we review some of the techniques copy-paste tampering detection.

Fridrich et al.[11] have made the first attempt for copy-paste tampering detection. Popescu and Farid[12] have further improved the algorithm and presented a method using principal component analysis (PCA). Myna et al.[13] developed a method for detecting and localizing copy-move forgery using a log-polar coordinates and wavelet transforms. Bayram et al.[14] use the Fourier-Mellin Transform (FMT), which involves a log-polar mapping, to represent image blocks. Li and Yu[15] extended the work performed by Bayram et al.[14], which is based on FMT. The authors[16] have

proposed a method in which the detection tampering depends on the correlation coefficient of the feature vectors of the blocks.

Most of the algorithms in Copy-Paste detections uses lexicographic sorting method to sort the feature vectors, but due to its computationally intensive nature, many authors[17,18,19] have used KD-tree as an alternative to it. The time complexity of lexicographical sorting was further improved by Lin et al.[20] which uses radix sort algorithm to sort row-wise feature vectors. Though, the time complexity was reduced, but the main limitation of radix sorting that it works only for integer type features; remains. The authors[21] have suggested using Krawtchouk moments to detect tampering with high accuracy. In[22], authors, propose a method in which texture of the segmented image blocks ascertains the tampering. Another approach in[23], the author uses Discrete Cosine transformer (DCT) as an effective way to reduce the computational cost of copy-move forgery detection. By comparing the developed method with the previous approaches, it is more efficient than the other.

The authors[24], uses Discrete Wavelet Transform (DWT) and Fast Walsh-Hadamard Transform. In[25], the dimension of an image is first reduced by applying DWT, and then spatial offset between copied portions are estimated by computing the phase correlation and detects forged regions. Li et al.[26] used DWT and SVD for feature vector reduction. The features are calculated using the approximation sub-band coefficients for block based DWT. In[27], dyadic wavelet transform, and statistical measures are used to detect the similar image segments from an image. In an another approach[28], the author uses the sub-blocking method. In an article[29], authors proposed the Zernike moments based Copy-Paste detection, the detection of the forged regions is found to be accurate.

Recently, Cozzolino et al.[30] proposed a fast copy-move forgery detection based on modified PatchMatch algorithm[31] with Zernike moments. To avoid feature matching a block clustering approach was proposed by an author[32]. Zandi et al.[33], proposed the use of an adaptive similarity threshold in the block-based feature matching stage. The author[34], the author, proposed a scheme based on dense nearest neighbor fields (NNF) and fast PatchMatch search algorithm. Cao et al.[35] proposed a technique for both global and local contrast detection in digital images using histogram peak/gap artifacts analysis. The author's[36] proposed an efficient algorithm for image inpainting detection.

The authors[37] applied histogram of orientated gradients to each block and lexicographic sorting to detect tampering. It is robust to distort by translation in small amount but not completely transformation invariant. Authors,[38] proposes a DCT based algorithm. It uses low frequency four and six coefficients of DCT of 8×8 pixel blocks. The author[39,40] uses three-step search algorithm of the motion estimation and subsampling in spatial domain method to reduce the size of the image and computational complexity. However, it is not robust to scaling and rotation.

Though, all the proposed methods in the literature work well in detecting copy-paste tampering. Almost all of them have two common problems: first is the computational cost and second is the low accuracy. Also, most of them fails to detect if the forged region had been rotated and scaled. The proposed algorithm in this paper is scale invariant. It is also rotation invariant to some extent of +3 to -3 degrees and do not need any feature vectors to be sorted. Hence, it is not necessary to perform lexicographic sorting, radix sorting or KD-tree; and NCC alone can be used for feature detection and matching. Hence, it is computationally efficient.

3. Normalized Cross Correlation

In this proposed method, we use Normalized Cross Correlation[41] (NCC) as a fundamental tool for feature matching. Matching two images of the similar scene is one of the fundamental problems in computer vision. Image matching plays a significant role in many applications such as image registration, motion analysis, stereo vision and mosaicking. In the last few decades, the image matching issue has been studied extensively, and several matching algorithms have been proposed[42,43] in computer vision.

The NCC is one of the basic and popular statistical approach used for image registration. It is widely used for template matching and pattern recognition. NCC is utilized as a metric to assess the level of dissimilarity or similarity between two signals or digital images. It is also advantageous to the simple cross-correlation because, it is robust to linear changes in the illumination amplitudes in the two compared images. Furthermore, the NCC is confined in the range between 1 and -1. The setting of detection threshold value is much simpler than the cross-correlation. Mathematically the NCC is given as:

$$C(x,y) = \frac{\sum_{y'=0}^{h-1}\sum_{x'=0}^{w-1} T(x',y')I(x+x',y+y')}{\sqrt{\sum_{y'=0}^{h-1}\sum_{x'=0}^{w-1} T(x',y')^2 \sum_{y'=0}^{h-1}\sum_{x'=0}^{w-1} I(x+x',y+y')^2}} \quad (1)$$

Where *(x',y')* are the template, *T*, coordinates, (*x, y*) are the Image, *I*, coordinates, and *h* and *w* are the height and width of the template. This metric computes pixel-wise cross-correlation and normalizes it by the square root of the auto-correlation of the images.

Instead of using the Matlab's library function for NCC, we have implemented our own, with some parameter customizations. The idea is to divide the image into large sized blocks and find the correlation between the image and these blocks. The threshold T_s, T_c, and T_f are set for detecting the scaling, coarse tampering and fine-tuned tampering respectively. Correlation between image and the image block is calculated. In case, if a strong correlation exists, then the correlation coefficient's value will be 1 or tends to be 1. The choice of the threshold parameter to be set is critical and important. Threshold with a very small value, i.e., nearer to zero and very high value as one may lead to wrong results. The threshold can take values between 0.85 to o.98. Once the values of T_s, T_c and T_f are set, it works for most of the cases without fail.

4. Proposed Method

The proposed Copy-Paste tampering detection method is based on block matching approach and uses NCC. As it can detect simple and scaled regions, we name it CSP, i.e., Copy-Scale-Paste tampering detection. It consists of three main steps.

1) Percentage of Scaling Detection
2) Coarse Scale Tampering Detection (CSTD)
3) Fine-Tuned Scale Tampering detection (FSTD)

Let '*I*' be the Image of size *W*×*H*, where *W*=width of the width of the image and *H*=height of the image.

Let '*B*' be the block of size *M*×*N* where *M*=width of block and *N*=height of the block.

Let S_h and S_v are the horizontal and vertical step size respectively. If step size in horizontal and vertical is same, then the common step size will be '*S*', i.e., $S=S_h=S_v$; and for the non-overlapping blocks $S_h=M$ and $S_v=N$. The total number of blocks can be formulated as:

$$NOB = \left[\left(\frac{W-M}{S_h}\right)+1\right] \times \left[\left(\frac{H-N}{S_v}\right)+1\right] \quad (2)$$

Divide the image into the overlapping blocks of size *M*×*N* and with a step size of S_h and S_v; if S_h and S_v same then, say $S_h=S_v=S$. *Let* τ_s is the threshold set for finding the scaling percentage.

The image is first divided into the *NOB*. Step size S_h and S_v decides the degree of block overlapping. To achieve efficiency and precision in the tampering detection, we have developed a 3-stage algorithm. The first stage is to detect the percentage of scaling. This is the main critical stage in the proposed method. Once the scaling factor is detected successfully, the Coarse Scale Tampering detection (CSTD) is done and the output of the second stage is i.e. CSTD is used to Fine-tune Scale Tampering detection (FSTD).

4.1. Percentage of Scaling Detection

This is the most important step as rest of the procedure will rely on the percent scaling returned by this algorithm. Here, there reference image ***I*** is divided into ***NOB***, the number of blocks. Rescale each block into different scales from 1% to 200%. Set the matching threshold for correlation. Calculate the correlation of the scaled block with the image. If the correlation is greater or equal to the set threshold, then stop the further processing and return the scaling percentage. Else continue processing till all the blocks of the image with different scaling ends. The algorithm is summarized in the following steps.

// C_B is the collection of overlapping blocks; τ_s threshold to detect percentage of scaling; ϕ is the scale factor
Get_Scale_Factor(I, C_B, NOB)
For each block B_i of C_B, where i=1, 2, 3,……, NOB
For each Scale factor ϕ = 0.01 to 2 in step of 0.01
B_{ir}=Scale b_i by ϕ
C_{oc}=Get the NCC of B_{ir} and image I
If C_{oc}>= τ_s
Return the ϕ
End
End
End

4.2. Coarse Scaled Tamper Detection (CSFD)

This is the second step and detects initial tampering. CSTD detects rough tampered areas. In this step, the block size chosen is very large. The choice made about the horizontal and vertical step size for dividing the image into blocks directly affects the results. Hence, choosing the step size for dividing an image is crucial. If the step size is large, then the processing will be fast but the tamper detection gets affected drastically, and method may fail to detect tampering, on the contrary, if the step size chosen is small then the block processing will take more time, but it increases the precision of tamper detection. The same is true for the block size also. Coarse regions of the tampering are detected based on the computation of the correlation matrix. Each coarse block is scaled by an amount of the detected scaling factor, and the correlation is calculated using equation 1. The decision on the matched blocks is taken based on the set $\boldsymbol{\tau_s}$. The locations of these detected blocks are recorded for further use. The steps of the algorithm is as follows.

Coarse_Scaled_Tamper_Detection(B, ϕ)
For each block B_i where i=1, 2, 3,……, NOB
B_{is}=Scale b_i by ϕ
C_{oc} =Get the NCC of B_{is}
If C_{oc}>= τ_s
Save the coordinates of the block B_i and scaled block B_{is}
Mark the coarse tampering
End
End
End

4.3. Fine-Tuned Scaled Tamper detection (FSTD)

As discussed earlier this step detects the tampered regions precisely. Each detected coarse blocks are divided into the small size blocks, and the NCC is carried out on the corresponding coarse block. If the threshold set for fine tuning stage is met, the match is considered, and final shape of the tampering is detected. The same procedure is repeated for all other blocks as well. The pseudo-code of the procedure is given below.

FineTuned_Scaled_Tamper_Detection(B, Bs)
For each B and B_s
Divide B and B_s into small blocks of size m×n, with a step size of s;
C_{oc}=Get the NCC of each small block of B and B_s sub-images
If C_{oc}>τ_f
Then highlight the Fine-tuned area.
Else
Skip the block and continue

End

End

5. Experimental Results

Several images from the CoMoFoD[44] database are tested to evaluate the performance of the proposed algorithm. The experimental results on few images from the CoMoFoD database are shown in Fig. 1 as shown below.

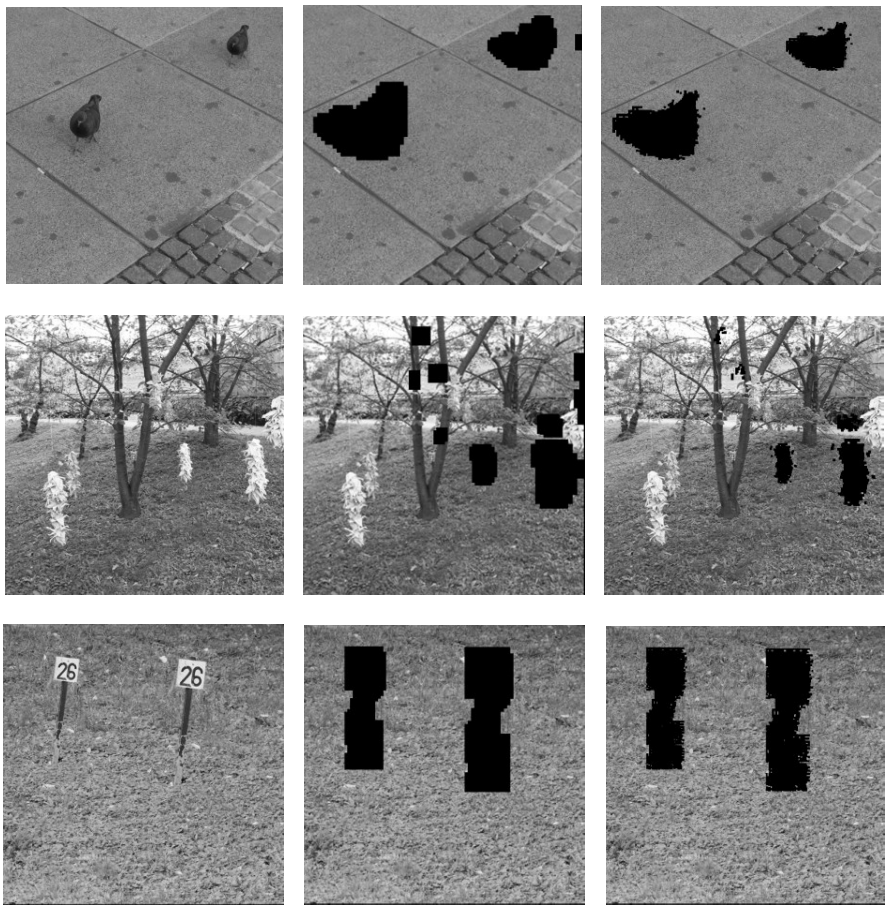

Fig. 1. (a) Original images from CoMoFoD database with scaled Tampering; (b) Coarse Scale Tamper Detection (CSTD) results; (c) Fine-tuned Scale Tamper detection (FSTD) results.

The experiments were carried out on a computer with a configuration of CPU Intel® Core i-5-4200M CPU @ 2.50GHz with 4.00GB Installed Random Access Memory on 64-bit Windows Operating System. The well-known CoMoFoD (Image Database for Copy-Move Forgery Detection for image forensics) is used to test the algorithms. The dataset consists of 260 forged image sets in two categories (small 512×512, and large 3000×2000). Images are grouped in five groups according to applied manipulations: rotation, translation, scaling, combination, and distortion. Various types of postprocessing methods, such as JPEG compression, blurring, noise adding, color reduction, etc., are applied to all forged and original images. We have used small 512×512 images for carrying out the tests. Tests are performed with different parameter settings, like threshold, coarse block size, the degree of overlapping, etc. The Coarse block size chosen was 24×24, and the step size chosen is 4. The threshold set for

detecting the scaling, finding the correlation of the coarse blocks and fine-tuning is 0.8, 0.9, 0.94 respectively. The following results show that the proposed algorithm detects the copied and the pasted regions successfully. The proposed algorithm was implemented using Matlab.

6. Conclusion

In this paper, we address the detection of copy-paste tampering in digital images. It is a popular image tampering technique among the forgers. We have proposed an efficient method to detect tampering in images efficiently and automatically. From the experimental conducted and the results obtained thereof, it has been observed that the NCC alone can perform well in detecting the tampering in images, even after transformation such as scaling. Moreover, no matter how much the size of the tampering area is, the forensics scheme can roughly detect those areas. The proposed method does not need dimensionality reduction and any sorting scheme to sort feature vectors and hence becomes computationally efficient as compared to some of the other block-based approaches in the literature. The proposed method is robust to the rotation to some extent but is not fool-proof to a rotation that needs to be addressed in future work.

References

1. The Internet Organised Crime Threat Assessment (iOCTA) [Internet]. Hague: Europol's European Cybercrime Centre (EC3); 2015 Oct. Available from: https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf
2. Kizza JM. Computer and Network Forensics. In: Guide to Computer Network Security. Springer; 2015. p. 299–324.
3. Danube Adria Association for Automation & Manufacturing, Katalinić B, Buchmeister B, Geršak J, DAAAM International (Vienna), editors. DAAAM International scientific book 2014. Vienna: DAAAM International Vienna; 2014.
4. Čisar P, ČISAR SM. General Directions of Development In Digital Forensics. Acta Tech Corvininesis-Bull Eng. 2012;5(2).
5. Karie NM, Venter HS. Toward a General Ontology for Digital Forensic Disciplines. J Forensic Sci. 2014;59(5):1231–41.
6. Dehnie S. Digital image forensics for identifying computer generated and digital camera images. In: Image Processing, 2006 IEEE International Conference on. IEEE; 2006. p. 2313–6.
7. Warbhe A, Dharaskar R, Thakare V. Block Based Image Forgery Detection Techniques. Int J Eng Sci Res Technol. 2015;4(8):289–97.
8. Farid H. Image forgery detection. Signal Process Mag IEEE. 2009;26(2):16–25.
9. Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E. An evaluation of popular copy-move forgery detection approaches. Inf Forensics Secur IEEE Trans On. 2012;7(6):1841–54.
10. Qureshi MA, Deriche M. A bibliography of pixel-based blind image forgery detection techniques. Signal Process Image Commun. 2015;39:46–74.
11. Fridrich AJ, Soukal BD, Lukáš AJ. Detection of copy-move forgery in digital images. In: in Proceedings of Digital Forensic Research Workshop. Citeseer; 2003.
12. Farid A, Popescu A. Exposing digital forgeries by detecting duplicated image regions. Technical Report, TR2004-515, Department of Computer Science, Dartmouth College, Hanover, New Hampshire; 2004.
13. Myrna A, Venkateshmurthy M, Patil C. Detection of region duplication forgery in digital images using wavelets and log-polar mapping. In: Conference on Computational Intelligence and Multimedia Applications, 2007 International Conference on. IEEE; 2007. p. 371–7.
14. Bayram S, Sencar HT, Memon N. An efficient and robust method for detecting copy-move forgery. In: Acoustics, Speech and Signal Processing, 2009 ICASSP 2009 IEEE International Conference on. IEEE; 2009. p. 1053–6.
15. Li W, Yu N. Rotation robust detection of copy-move forgery. In: Image Processing (ICIP), 2010 17th IEEE International Conference on. IEEE; 2010. p. 2113–6.
16. Kang L, Cheng X. Copy-move forgery detection in digital image. In: Image and Signal Processing (CISP), 2010 3rd International Congress on. 2010. p. 2419–21.
17. Langille A, Gong M. An efficient match-based duplication detection algorithm. In: Computer and Robot Vision, 2006 The 3rd Canadian Conference on. IEEE; 2006. p. 64–64.
18. Christlein V, Riess C, Angelopoulou E. A Study on Features for the Detection of Copy-Move Forgeries. In: Sicherheit. 2010. p. 105–16.
19. Mahdian B, Saic S. Detection of copy–move forgery using a method based on blur moment invariants. Forensic Sci Int. 2007;171(2):180–9.
20. Lin H-J, Wang C-W, Kao Y-T, others. Fast copy-move forgery detection. WSEAS Trans Signal Process. 2009;5(5):188–97.
21. Imamoglu MB, Ulutas G, Ulutas M. Detection of copy-move forgery using krawtchouk moment. In: Electrical and Electronics Engineering (ELECO), 2013 8th International Conference on. IEEE; 2013. p. 311–4.
22. Quan X, Zhang H. Copy-move forgery detection in digital images based on local dimension estimation. In: Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on. IEEE; 2012. p. 180–5.
23. Kumar S, Desai J, Mukherjee S. A fast DCT based method for copy move forgery detection. In: Image Information Processing (ICIIP), 2013 IEEE Second International Conference on. IEEE; 2013. p. 649–54.

24. Yang B, Sun X, Chen X, Zhang J, Li X. An Efficient Forensic Method for Copy–move Forgery Detection based on DWT-FWHT. Radioengineering. 2013;22(4).
25. Zhang J, Feng Z, Su Y. A new approach for detecting copy-move forgery in digital images. In: Communication Systems, 2008 ICCS 2008 11th IEEE Singapore International Conference on. IEEE; 2008. p. 362–6.
26. Li G, Wu Q, Tu D, Sun S. 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. IEEE; 2007. p. 1750–3.
27. Muhammad N, Hussain M, Muhammad G, Bebis G. Copy-move forgery detection using dyadic wavelet transform. In: Computer Graphics, Imaging and Visualization (CGIV), 2011 Eighth International Conference on. IEEE; 2011. p. 103–8.
28. Singh VK, Tripathi R. Fast and efficient region duplication detection in digital images using sub-blocking method. Int J Adv Sci Technol. 2011;35:93–102.
29. Mohamadian Z, Pouyan AA. Detection of Duplication Forgery in Digital Images in Uniform and Non-uniform Regions. In: Computer Modelling and Simulation (UKSim), 2013 UKSim 15th International Conference on. IEEE; 2013. p. 455–60.
30. Cozzolino D, Poggi G, Verdoliva L. Copy-move forgery detection based on patchmatch. In: Image Processing (ICIP), 2014 IEEE International Conference on. IEEE; 2014. p. 5312–6.
31. Barnes C, Shechtman E, Goldman DB, Finkelstein A. The generalized patchmatch correspondence algorithm. In: Computer Vision–ECCV 2010. Springer; 2010. p. 29–43.
32. Sekeh MA, Maarof MA, Rohani MF, Mahdian B. Efficient image duplicated region detection model using sequential block clustering. Digit Investig. 2013;10(1):73–84.
33. Zandi M, Mahmoudi-Aznaveh A, Mansouri A. Adaptive matching for copy-move Forgery detection. In: Parallel Computing Technologies (PARCOMPTECH), 2015 National Conference on. IEEE; 2015. p. 119–24.
34. Cozzolino D, Gragnaniello D, Verdoliva L. Image forgery detection through residual-based local descriptors and block-matching. In: Image Processing (ICIP), 2014 IEEE International Conference on. IEEE; 2014. p. 5297–301.
35. Cao G, Zhao Y, Ni R, Li X. Contrast enhancement-based forensics in digital images. Inf Forensics Secur IEEE Trans On. 2014;9(3):515–25.
36. Liang Z, Yang G, Ding X, Li L. An efficient forgery detection algorithm for object removal by exemplar-based image inpainting. J Vis Commun Image Represent. 2015;30:75–85.
37. Lee J-C, Chang C-P, Chen W-K. Detection of copy–move image forgery using histogram of orientated gradients. Inf Sci. 2015;
38. Shin Y-D. Fast Detection of Copy-Move Forgery Image using DCT. J Korea Multimed Soc. 2013;16(4):411–7.
39. Shin Y-D. Fast detection of copy-move forgery image using three step search algorithm in the spatial domain. In: Convergence and Hybrid Information Technology. Springer; 2012. p. 389–95.
40. Shin Y-D. Fast detection of Duplicated Forgery Image using Sub-sampling. J Converg Inf Technol. 2015;10(2):17.
41. Lewis J. Fast normalized cross-correlation. In: Vision interface. 1995. p. 120–3.
42. Zitova B, Flusser J. Image registration methods: a survey. Image Vis Comput. 2003;21(11):977–1000.
43. Brunelli R. Template matching techniques in computer vision. Wiley; 2008.
44. Tralic D, Zupancic I, Grgic S, Grgic M. CoMoFoD—New database for copy-move forgery detection. In: ELMAR, 2013 55th International Symposium. IEEE; 2013. p. 49–54.