International Journal of Advanced Science and Technology
Vol. 29, No. 9s, (2020), pp. 5199-5206

Nonlinear Approximated Regression of Holistic Feature for Copy Move Forgery Detection

Punam Sunil Raskar[1], Sanjeevani K. Shah[2]

[1]*Research Scholar, Sinhgad College of Engineering (E&TC),Savitribai Phule Pune University, Pune, India*
[2]*Professor, Smt. Kashibai Navale College of Engineering (E&TC),Savitribai Phule Pune University, Pune, India*

Abstract

Due to advance operational editors, digital images and videos can be tampered very easily. These forged/fake images and videos communicated across the world through various apps over social media.Tamperingin video is a common problem facing by all over the world which causes the negative impact on society. Numerous methods have been proposed to detect altering in videos. Techniques for video tamper detection broadly categorised according block division operation and key point feature extraction. This paper aims to propose a low computational technique to discover copy-move attack in videos. An improved BHFD (Blockwise Holistic Feature Descriptor) and SVR technique is proposed to object based copy-move detection within the video frames. Holistic Gabor descriptor is used for feature extraction and SVR (Support Vector Regression) training is used for classification of forged and non-forged video frames. Experimental analysis and results demonstrates proposed system woks satisfactorily for handcrafted videos with reduced computational complexity.

Keywords: *BHFD, Copy-move forgery, Nonlinear Approximation, SVR.*

1. Introduction

Videos are extensively used and important in many areas. They have become part of everyday life as well as part of many applications in science. Due to current development in mobile application and social media communication use of video and images is increased rapidly. There are many apps available online and on play store. This makes forging in video without any visible traces easier. Copy-move forgery in an image or video is extensively used image manipulation scheme. In this type of forgery, some image region is copied and pasted into the same image or in a video frame. As the fake imagearea comes from the same image or video, the spatial characteristic of image remains largely same, which increases the difficulty of detecting this type of image forgery. In the past, several attempts of image altering have been exposed [16].Simple and free to usemobile apps and image editing software's provides key to produce object forgeries. Consequently the semanipulated images creates confusion to make judicial decision. Hence, confirmingthe authenticity of digital images is prime essential and makes important role in forensic department [10]. Forensic unitmake use of advanced skill and techniques to examineevidence in courts for criminal circumstances [11, 12] as well as in areas, where the authenticity of the digital image is important such political and sports frauds in courtrooms, banking sectors, biometric imaging etc.[13-15].

Image/Video forgery is a widely studied research today as, forgery detection in digital images and videos is gaining enormous attention to provide security to digital media from several tampering skills and forgery attacks.This exertion is significant in forgery detection architecture and can be utilized for high security associationsTamper localization and detection techniques in video frames identifies the tampered frame correctly by means of temporal or inter frame passive techniques whereas intra frame methods or spatial characteristics of the video discovers altered contents within the forged frame. When a video is altered, the geometricfeatures of the frame correspondingly changes.However, if video forgery is done with precaution, without leaving any evidence, then it is very difficult for an expert to recognise whether this video is original or forged. Prevailing methods for copy move forgery recognition can be grouped into two classes, for example block-based and key point-based techniques. The methods based on block division, as a rule extract details from covering blocks of the image.Various highlights have been suggestedby taking benefit of this type for the recognition of forgeries in an image or video. Whereas second class uses key point features of image or frame which helps in detecting tampering in image of videos.

ISSN: 2005-4238 IJAST

Figure 1.General process pipeline for the copy-move forgery detection in video

Most of these approaches follow a generalstages as shown in Fig. 1. The pipeline comprises threesteps: 1) Frame Conversion: In this steps video is splitinto frames according to its frame rate. 2) Feature Extraction: In this stage texture or key point based features are extracted from image or it is extracted from block wise processing.3) Feature Matching: In this step extracted features are compare with previously extracted features. If the extracted distance is matched with some threshold then at that location forging is done.

The key contributions of this paper addresses few issues such as:Proposed method primarily stated to detect duplications in video.Moreover, wehave tried to optimize the feature extractionand feature matching process, which improve the computational efficiency significantly. Proposed algorithm suggests improvementin two aspects by the optimization of features using Holistic descriptor and Nonlinear approximation in traditional SVR to increase its accuracy metric. Also, proposed algorithm is designed to achieve the detection of multiple copy-move regions in real-time applications.

The paper is structured as follows. Section I provides introduction. Section II highlights on various research on copy move forgery. Section III contributes proposed method, Discussion on various experimentation is explained in section IV. Section V concludes the finding of proposed method.

2.Related Work

The purpose of copy-move attack detection is to identify the forged (copied) part with minor changeswith original part. Lots of research is done on image and it is continuously increasing in this area of tamper detection. However, in real time application, intra frame or copy-move forgery is carried out with various types of image basic pre-processing, which involve spatial manipulation such as rotation, scaling, mirroring, or colour based operations such as illumination alteration, or chrominance, luminance alteration. Some other manipulation are copied region enhancement such as sharpening or blurring.

Subjective survey of copy move image imitation identification methods has been explained and in this section. Image imitation detection has been categorised into different methods. Fredrich, et al. [1] suggested a technique based on DCT, in which block wise matching is carried out also it works only for small windows. Popescuet al. [2] recommended Principal Component Analysis (PCA) based technique. This blockwise PCA found robust to small manipulation for copied region.Ascheme based on Local Binary Pattern (LBP) and clustering, which works on colour histogram based features to detect the forged region is proposed by Al-Sawadi et al. [3]. This method was vulnerable to Rotation and scaling. Bayram, et al. [4], proposed a technique to discover forgery by using Fourier-Mellin Transform (FMT). As this method is depend on block wise Fourier transform, it was robust to small degree of rotation and scaling.Muhammad, et al. [5], stated techniques using un-decimated Dyadic Wavelet Transform (DyWT). In this method due to decomposition, forged part detection becomes easy and robust. Zhong and Xu [6], proposed architecture based on mixed moments in which fourier moments are estimated blockwise. This method works for detection of part with intensity change.Hussain et al. [7], states method based on a multi resolution Weber local descriptor (WLD) system with shape invariant features. Amerini et al. [8] states a Scale Invariant Feature Transform (SIFT) based method. This method works better for scale androtationinvariant.Hashmi, et al. [9], developed architecture using (DyWT) and (SIFT), which ensures better detection rates.

ISSN: 2005-4238 IJAST

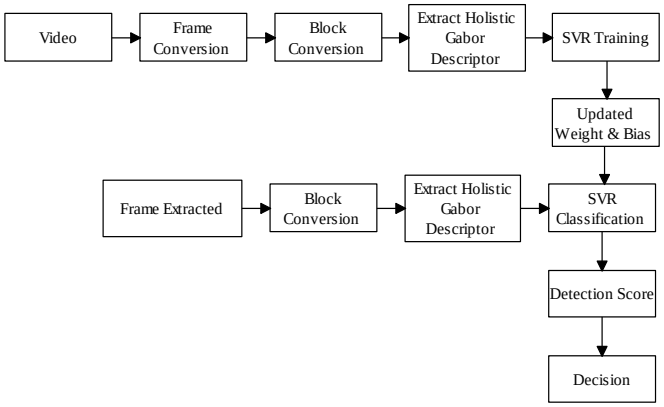

Figure 2.Proposedholistic Feature Approach Architecture

3.Proposed Methodology

Figure 2 describes proposed architecture. Initially input video is converted into frames. Then frame by frame and block by block image features are extracted. Here, for experimental purpose block size selected is 64x64.Blockwise Holistic feature descriptor is used for extraction for the same. After feature extraction of each block SVR classifier training is conducted.

A. Blockwise Holistic Feature Descriptor (BHFD)

Recently, number of various approaches have been developed to improve feature extraction for forgery detection. One of the most successful strategies has shown to be the use of Gabor representation of the images. BHFD features is an extension of holistic feature descriptor, in which image is processed batch wise. The Gabor channel (Gabor Wavelet) states to a band-pass direct channel whose motivation reaction is characterized by a symphonies capacity increased by a Gaussian capacity. Along these lines, a bi-dimensional Gabor channel creates a multifaceted sinusoidal plane of particular recurrence and direction adjusted by a Gaussian envelope. Gabor features are popularly renowned for effective representation. But, only some of the methodsexploit phase feature and they generallyachieve worse than those using magnitude feature. For this reason, only the blockwise magnitudes of the Gabor coefficients are thought of as being useful for feature extraction. It accomplishes an ideal goal in both spatial and recurrence areas. Our methodology structures 2D odd-symmetric Gabor filter, having the accompanying structure as stated in equation (1)

$$HD(F)_{\theta_k, f_i, \sigma_x, \sigma_y}(x,y) = exp\left(-\left[\frac{x_{\theta_k}^2}{\sigma_x^2} + \frac{y_{\theta_k}^2}{\sigma_x^2}\right]\right).\cos(2\pi f_i x_{\theta_k} + \varphi) \quad (1)$$

B. Support vector regression (SVR)

Let consider that a calculated feature coefficient of up till visited object $\{(x_1, y_1), ..., (x_l, y_l)\} \in x_i$ where x_i denote the feature extracted from previously visited block and y_i denote thetarget which is ones or zeros depending upon distance threshold. The support vector regression model is to find $y = \langle \omega, \phi(x) \rangle H + b,$

ω and $\phi(x)$ are the feature space estimated from Kernel Hilbert space H. SVR can be optimised by,

$$R = \frac{1}{2}\|\omega\|^2 + c\sum_{i=1}^{l} L(y_i, x_i, f). \quad (2)$$

Where L (y_i, x_i, f) denotes the $\in$- loss function given by

$$L(y_i, x_i, f) = |y - f(x)|_{\in} = \max(0, |y - f(x)| - \in) \quad (3)$$

$$\min_{\omega, b, \xi, \tilde{x}i} \frac{1}{2}\|\omega\|^2 + c\sum_{i=1}^{l}(\xi^2 + \tilde{\xi}^2) \quad (4)$$

$$\begin{cases} f(x_i) - y_i \le \in +\xi_i, i = 1,...,l \\ y_i - f(x_i) \le \in +\xi_i, i = 1,...,l \\ \xi_i, \tilde{\xi}_i \ge 0 \end{cases}$$

Subject to

Solution can be achieve using Lagrangiantheory :

$$\omega = \sum_{i=1}^{l} (\hat{\alpha}_i - \alpha_i) \phi(x_i), \tag{5}$$

Where $\{\hat{\alpha}, \alpha\}, i = 1,...,l$ are the Lagrangianco efficient.

it can be optimised by following criteria,

$$\max_{\alpha_i, \hat{\alpha}_i} \sum_{i=1}^{l} y_i (\hat{a}_i - \alpha_i) - \in \sum_{i=1}^{l} (\hat{a}_i + \alpha_i) - \frac{1}{2} \sum_{i,j=1}^{l} (\hat{a}_i - \alpha_i)(\hat{a}_j - \alpha_j)$$

$$\left(K(x_{i,} x_j) + \frac{1}{c} \zeta i, j \right) \tag{6}$$

Subject to

$$\left\{ \sum_{i=1}^{l} (\hat{\alpha}_i - \alpha_i) = 0 \right.$$

$$\left\{ 0 \le \alpha_i, 0 \le \hat{\alpha}_i, i = 1, \ldots, l, \right.$$

Where $K(x_i, x_j) = \langle \phi(x_i), \phi(x_j) \rangle H$ and $\zeta_{i,j}$ are Kroneckerco efficient.

Algorithm 1: Feature matching based on SVR

Procedure SVR(X,Y)

$X_i = \{x_1, x_2, ..., x_N\}, Y_i = \{y_1, y_2, ..., y_N\}$

$X = \left[X_{i,1}, X_{i,2}, ..., X_{i,D} \right]^T, Y = \left[Y_{i,1}, Y_{i,2}, ..., Y_{i,D} \right]^T, u = \left[X, Y \right]^T,$

$E(\theta, \sigma | X_i)$ and $E(\theta, \sigma | Y_i)$

for $k \leftarrow 1, K$ do

for $i \leftarrow 1, \mathrm{I}$ do

for $b \leftarrow 1, B$ do

$X_{i,b}^* = \{x_1^*, x_2^*, ..., x_N^*\}$ and $Y_{j,b}^* = \{y_1^*, y_2^*, ..., y_N^*\},$

$\bar{X}_{i,b}^* = \frac{1}{N} \sum_{n=1}^{N} x_n^*$ and $\bar{Y}_{i,b}^* = \frac{1}{N} \sum_{n=1}^{N} y_n^*,$

$X_i^* = \{\bar{x}_{i,1}^*, x_{i,2}^*, ..., \bar{x}_{i,B}^*\}$ and $Y_i^* = \{\bar{y}_{j,1}^*, \bar{y}_{j,2}^*, ..., \bar{y}_{j,B}^*\}$

end for

end for

SVR $\left\{ \hat{f}^{*k} (X_i^*, Y_i^*) \right\}$

end for

$\hat{f}_{\varphi}(.) = \mathrm{K}^{-1} \sum_{k=1}^{K} \left(\hat{f}^{*k} (X_i^*, Y_i^*) \right)$

Output: weights and biases to fine-tune

end procedure

Thus, block division is carried out of complete image as a first step of proposed scheme. Then from each image block features are pulled out. These extracted features are the then compare with the previous block wise extracted features. If the features are found with some similarity i.e with minimum distance from hyperplane then those part is

detected as a forged on. SVR will be best approach for such approach as it have capability to handle the nonlinearity in the shape, scale, or other transformation.

4.Experimental Results

Proposed method is tested and implemented for 15 videos. All videos for experimental analysis are taken from MATLAB Vision demos. Further these videos are forged by applying copy move attack on random frame using adobe Photoshop editor. Environment used for proposed method conduction is MATLAB 2018. Hardware Core i5 processor with 4GB memory.

Figure 3 (a) is original video frame. This frame is forged by applying copy-move forgery, tree on left hand upper corner of person's head is copied and it is paste in right upper corner. An upper right corner already has one tree is present. This tree portion is masked with newer one as shown in figure (b). Figure (c) shows detected forged part within the frame (shown by yellow colour rectangle).

(a) (b) (c)

Figure 3(a) Original video frame (b) Forged Frame by Copy-Move attack (c) Forged frame (Forged part shown by yellow rectangle)

(a) (b) (c)

Figure 4.(a) Original video frame (b) Forged Frame by Copy-Move attack (c) Forged frame (Forged part shown by yellow rectangle)

In Figure 4 (a) shows original frame having a single person. The person is copied and it is paste aside with already presented one shown in (b). Figure (c) shows Detected forged part highlighted by yellow colour.

Figure 5.Video frame of Original & Forged video

In Figure 5 white vehicle is copied from left image (Original frame) and it is paste in top row, this forged frame is shown on middle figure. Right figure shows Detected forged part displayed by yellow box.

Figure 6.Original Frame & Detected Forged Frame (yellow Color Rectangle)

In Figure 6 two vehicle is copied from left image (Original frame) and it is paste in top row, this forged frame is shown on middle figure. Right figure shows detected forged part highlighted by yellow box.

Comparative Analysis of Proposed System

Proposed method is designed to achieve the improved feature extraction and matching algorithm for the extraction of other image features, results for the same are provided in above section. For the comparisonof proposed method, experimentation were performed on 15 Videos at a resolution of 640 × 480 pixels. Clearly, the proposed algorithm is computationally better in terms of execution time than other methods stated for comparative scheme. Table 1 shows that proposed method exhibited the good performance amongst different state-of-art methods. From Table 1 graphical representation is shown in figure 7.

Table 1.Comparative analysis of the Execution Time

Video No	Wang[17]	S. V[18]	Pun[19]	Proposed
1	9.753621	6.498508	14.15045	6.522293
2	9.155437	7.882708	13.3592	6.608148
3	9.052927	7.620664	13.79945	5.236477
4	9.843122	7.379764	14.51173	5.059519
5	9.506868	7.525417	14.18898	5.653712
6	8.297023	6.748402	13.2584	5.076952
7	8.772467	7.870567	13.82776	5.05741
8	9.569301	6.598318	13.83916	5.816274
9	9.501779	6.746905	14.18834	6.132838
10	9.074575	7.886437	14.07196	5.56731
11	8.669126	7.130125	14.58135	6.165128
12	8.475009	6.535687	14.49771	5.42918
13	8.649843	7.835636	13.42417	5.583306
14	9.032783	6.872962	14.07195	6.384714
15	8.720366	7.548864	13.73059	6.256215

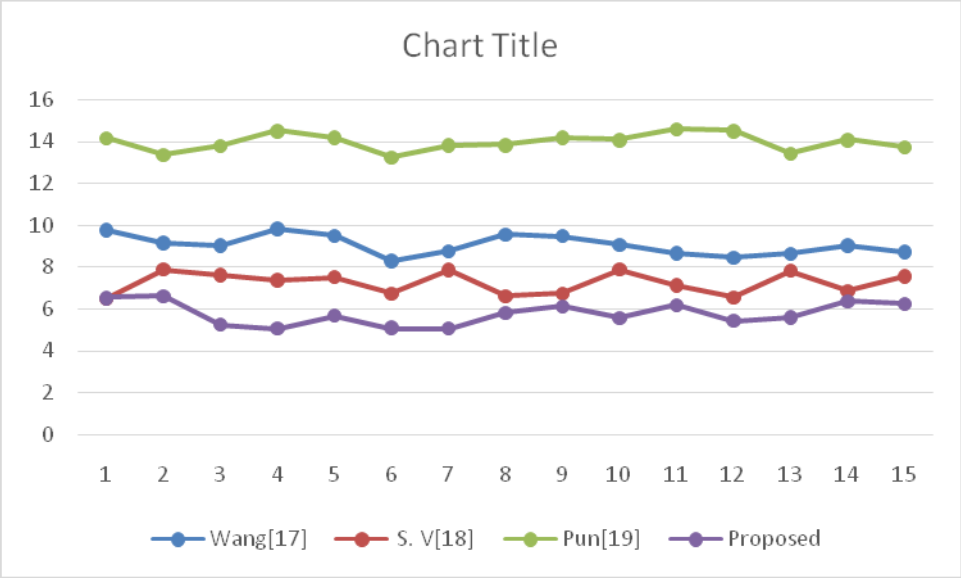

Figure 7 Comparison of Execution Time of Proposed method with existing

Performance of proposed system is measured by calculating various factors such as Accuracy, Recall rate, Specificity, Precision. The parameters are calculated by using confusion matrix formulae on the basis of TP (True Positive), FP (False Positive), TN (True Negative), FN (False Negative) values. Further we have compared these values with state-of-art methods as illustrated in Table 2.

Table 2 Comparative Analysis of Performance Metrics

P. M	Wang[17]	S.V[18]	Pun[19]	Proposed
Accuracy	0.96	0.94	0.93	0.98
Recall	0.8	0.7	0.6	0.9
Specificity	0.98	0.97	0.97	0.99
Precision	0.8	0.7	0.6	0.9

All the metrics is calculated in terms of block i.e. detected block is forged or not.Accuracy is block correctly classified as a forged and correctly classified as a normal out of total available blocks. Sensitivity is block correctly classified as a forged and out of total forged blocks. Specificity is block correctly classified as a Normal and out of total Normal blocks. Precision is block correctly classified as a forged and out of total predicted forged blocks and total normal block predicted as a forged. Figure 8 graphical representation of Accuracy, Recall, Specificity and Precision respectively.Accuracy for proposed method achieved is 98%, however other methods are variesfrom 93.5% to 96.5%. Recall of proposed method achieved is as 0.9 value, while other methods are having between the ranges 0.6 to 0.8. Similarly, Specificity and Precision of proposed method obtained as 0.99and 0.9 respectively.

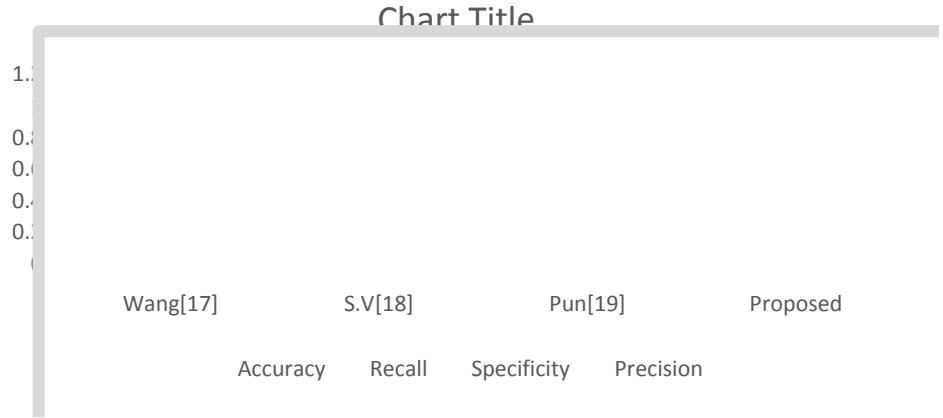

Figure 8.Graphical Analysis of Proposed method with existingfor a) Accuracy b) Recall c) Specificity d) Precision

5.Conclusion

Technique based on an improved BHFD and SVR based copy-move image forgery detection is proposed in this paper. The evaluation and experimentation of proposed approach is demonstrated on various forged videos. Investigationaloutcomes show that the proposed scheme better outperforms than the traditional-based method in reliability of detection and efficiency. Execution time required for proposed method is reduced to 50% on an average. Also, Accuracy for detection of the forged frame is increased 3% in comparison with various state-of-art method. Future work to is to try this technique on standard or benchmark datasets that purely belongs to forensic purpose.

References

1. Fridrich, J. Soukal, D. Luk, J. (2003), Detection of copy-move forgery in digital images, Proc. Digital Forensic Research Workshop, Cleveland, OH, USA.
2. Popescu, A. and Farid, H. (2004), Exposing Digital Forgeries By Detecting Duplicated Image Regions, Tech. Rep. TR2004-515, Dartmouth College, Computer Science, Hanover, Conn, USA.
3. Al-Sawadi, M. Mohammad, G. Hussain, M. Bebis, G. (2013), Copy-Move Image Forgery Detection Using Local Binary Pattern and Neighborhood Clustering, Modelling Symposium (EMS), 2013 European, (20-22 Nov. 2013), Manchester, pp. 249 – 254
4. Bayram, S. Sencar, T. Memon, N. (2009), An Efficient And Robust Method For Detecting Copy-Move Forgery," in Proceeding of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '09), pp. 1053–1056, Taipei, Taiwan.
5. Muhammad, G. Hussain, M. Bebis, G. (2012), Passive Copy Move Image Forgery Detection Using Undecimated Dyadic Wavelet Transform, Digital Investigation, vol. 9, pp. 49–57.
6. Zhong, L. and . Xu, W. (2013), A Robust Image Copy-Move Forgery Detection Based On Mixed Moments, in Proceedings of the 4th IEEE International Conference on Software Engineering and Service Science (ICSESS '13), pp. 381–384, IEEE.
7. Hussain, M. Muhammad, G. Saleh, S. Mirza, A. Bebis, G. (2012), Copy-Move Image Forgery Detection Using Multi-resolution Weber Descriptors, in Proceedings of the 8th International Conference on Signal Image Technology and Internet Based Systems (SITIS '12), pp. 395–401.
8. Amerini, I. Ballan, L. Caldelli, R, Bimboa, A. Tongoa, L. Serra, G. (2013), Copy-move forgery detection and localization by means of robust clustering with J-Linkage, Signal Processing: Image Communication, vol. 28, Issue: 6, pp. 659–669.
9. Hashmi, M. Anand, V. Keskar, A. (2014), Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform, 2014 AASRI Conference on Circuit and Signal Processing (CSP 2014), vol. 9, pp.84-91.
10. Barni M, Costanzo A (2012) A fuzzy approach to deal with uncertainty in image forensics. Signal Process Image Commun 27(9):998–1010
11. Battiato S, Farinella GM, Messina E, Puglisi G (2012) Robust image alignment for tampering detection. IEEE Trans Inf Forensics Secur 7(4):1105–1117
12. Lin HJ, Wang CW, Kao YT et al (2009) Fast copy-move forgery detection. WSEAS Trans Signal Process 5(5):188–197
13. Christlein, V., Riess, C., Jordan, J., Riess, C., &Angelopoulou, E. (2012). An Evaluation of Popular Copy-Move Forgery Detection Approaches. IEEE Transactions on Information Forensics & Security, 7(6), 1841-1854.
14. Huang, H., Guo, W., & Zhang, Y. Detection of copy-move forgery in digital images using SIFT algorithm. In Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on, 2008 (Vol. 2, pp. 272-276): IEEE
15. Sencar, H. T., &Memon, N. (2008). Overview of state-of-the-art in digital image forensics. Algorithms.
16. Kakar, P., N. Sudha, and W. Ser. (2011). Exposing Digital Image Forgeries by Detecting Discrepancies in Motion Blur. IEEE Transactions on Multimedia, 13(3), 443-452.
17. W. Wang and H. Farid, "Exposing digital forgeries in video by detecting duplication," in Proc. 9th workshop Multimedia Security, 2007, pp. 35–42.
18. Subramanyam, A. Venkata, and Sabu Emmanuel. "Video forgery detection using HOG features and compression properties." 2012 IEEE 14th International Workshop on Multimedia Signal Processing (MMSP). IEEE, 2012.
19. C.-M. Pun, X.-C. Yuan, and X.-L. Bi, "Image forgery detection using adaptive over segmentation and feature point matching," IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1705–1716, Aug. 2015.