Detection and Localization of Image and Video Tampering

Silpa Joseph, S.Palanikumar

***Abstract:** Digital images and videos are widely used in various fields like courtrooms ,military ,medicine ,research, social media etc. So, maintaining the authenticity and integrity of these digital contents is a major concern. For the past few years, researches were going on to find out tampering in the digital contents. Active and passive approaches are the major classification for digital tampering detection. Here, we discuss some of the active and passive approaches and their significance in the current scenario.*

***Keywords:** Digital Image Watermarking, Copy-move Forgery, Splicing, Singular Value Decomposition, Peak-Signal-to-noise ratio, Bit Error Rate, Scale Invariant Feature Transform, Group of Pictures,F1-Score etc.*

I. INTRODUCTION

Life in a modern society in which, people uses various gadgets, social media platforms and techniques with a mere knowledge about the technology behind them. People with malicious intent are able to capture digital images and videos with various devices, save, manipulate and transmit them through the different social media platforms. Here comes the importance of keeping the authenticity and integrity of these digital images and videos, since they can be utilized in various fields like courtrooms, military, research journals, medicine, media etc.

For the past few decades, digital forensics helps us to restore the lost trust on digital contents by detecting forgeries , identify the origin and tracing the processing history[1].Forgery detection and forgery localization are the two major issues in image forensics[2].The former checks only whether an image is genuine or counterfeit but the later deals with the localization of the forged region in a modified digital content. Previous research works were concentrated on forgery detection, but now the importance is given on localization of tampered images.

Active and Passive approaches are the two classifications of forgery detection techniques in images [3]. In active approach some additional information's are embedded along with the digital image during the capturing process or later by the authorized person, which is helpful in tampering detection. Active approach are again categorized into two: digital signature and digital watermarking. Digital signature deals with the authenticity of the images whereas digital watermarking is the technique of lodging some data in a digital content. Robust, fragile and semi fragile watermarking are the various classifications of digital watermarking. Tampering can be detected, if there is any change occurs on the embedded information. But images are captured by various devices that does not support these facilities, so the images may not contain this embedded information. The active approach detection techniques can be used only on digital images with this additional information and are not widely used like passive approaches.

On the other hand, the passive approach does not require any pre-processing. The manipulation detection in images is done by extracting their intrinsic features [3] based upon tampering detection and source device identification. The tampering detection can be again classified into dependent and independent approaches. The dependent method consists of copy-move forgery (copying and pasting the contents from the same image) and splicing (copying and pasting from different images).The independent method includes compression, re-sampling and inconsistencies. In source device identification the traces left behind by the digital cameras like sensor and optical fingerprints.

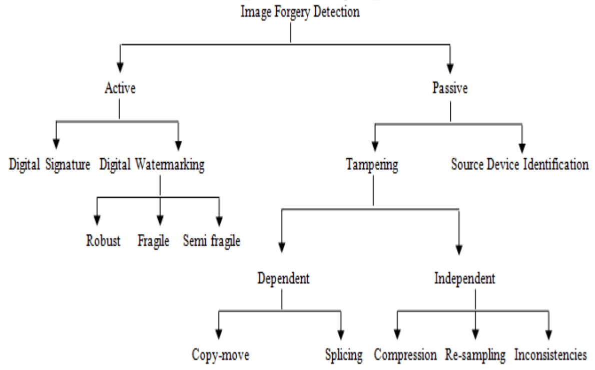


Fig.1-Image Forgery Detection Techniques

The Fig.1 represents various forgery detection techniques. In the next section II we dealt with numerous image and video tampering techniques based on this classification. Section A discusses on some of the fragile and robust watermarking techniques. Section B discusses on various copy-move and splicing techniques. Section C dealt with some of the fusion approaches and Section D consists of different video tampering detection techniques .Section III and IV discusses on the result analysis and conclusion.

II. DIVERSE TAMPERING DETECTION AND PROCESSING OPERATIONS

In various real time scenarios, the digital images and videos may contain many valuable information[1]. For example an image or video released by the government,

Revised Manuscript Received on February 06, 2020.
***** Correspondence Author

Silpa Joseph*, Research Scholar,,CSE , Noorul Islam Centre for Higher Education,Kumarakovil, India. Email: silpa.aji@gmail.com.

S.Palanikumar, Associate Professor ,department of IT, Noorul Islam Centre for Higher Education,Kumarakovil, India. Email:palanikumarcsc @yahoo.com

may have vital information's that may lead to political or societal consequences. So instead of blindly trusting these documents, we must ensure that they are authentic .In recent years various tampering detection techniques, are developed by the researchers. These techniques are operated by exploiting the features of the digital image contents itself.

A.DIGITAL IMAGE WATERMARKING

Digital Image Watermarking is an active approach that can be used to ensure the authenticity and integrity of an image. While transmitting some sensitive or critical information such as formal, legal, financial, medical and religious document [4],[5], we must ensure its credibility. Digital watermarking can be robust, fragile and semi-fragile based on their characteristics. Robust watermarking is useful in proving the ownership claims, which can resist various geometrical and non-geometrical attacks. It can withstand editing, image processing and digital compression. Fragile watermarking is very sensitive to the changes of signals and is used for multimedia content authentication. Semi fragile watermarking is capable to survive changes such as noise addition due to lossy compression on a watermarked image to some extent.

The previous techniques deals with only tampering detection[6]-[9], and faces problems like undetectable modifications, insecure block mappings ,localization failure and poor recovery quality. But the recent researches focus on both tampering detection and recovery of this tampered images [10]-[14].The work in [10] and [11] dealt with fragile watermarking and self recovery of digital images. A block-neighborhood tampering detection characterization and its performance analysis is done in [10] using the auto recovery fragile watermarking scheme on various attacks. Previously mentioned problems faced by various watermarking techniques and its vulnerability to constant-average attack were overcome by adding two secure key bits to each block. Satisfactory results were obtained for image recovery where image tampering was up to 60%.

In [11], Chinese Remainder Theorem based on fragile self-recovery watermarking scheme is used for tampering detection/recovery. Since the computations are done using modular arithmetic, the computational complexity is less in this method. It has shown improvement in both the capacity and intangible performance metrics, but very few attacks were only handled. In [15], they focus for medical applications, using fragile watermarking-based schemes for image authentication and self-recovery. Here the authentication bits are block authentication and self recovery bits which are later used to sustain from the vector quantization attack. Various attacks like text insertion and removal, copy paste attacks are handled by this technique. The work in [16] proposes a robust tamper localization method for sensitive images and documents. This method shows resistance to random paint-based and stirmark-based attacks for subtle documents with peak-signal-to-noise ratio of 43dB.

B.COPY-MOVE AND SPLICING

The copy-move forgery and splicing forgery is used to hide or generate some sensitive or fake information. This is one of the major research areas in the last few years. Hundreds of papers are published based on this field. Copy-move forgery dealt with copying content from an image and pasting to some other part of the original image itself, in order to hide some relevant information. The workflow of copy move forgery detection falls through four stages-pre-processing, extractions of features, matching and visualization. The starting stage is pre-processing, in which we suppress the unwanted distortions or enhance the image features to improve the image quality. This helps to reduce the complexity of the process and visual features of an image to be improvised. While in the next stage, ie feature extraction, the relevant information of an image that shows its characteristics is extracted. In the third stage, we search the similarities of these features.

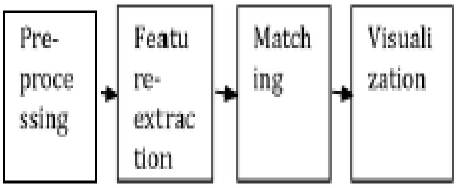


Fig.2-Workflow of copy-move forgery detection

The matching process can be done by two techniques-methods based on block and key point. In block based method the image is partitioned into rectangular patches and similar patches are found by sorting and thresholding techniques. But in the key point based method we extract some feature points from an image without any subdivisions. We localize and view the tampered image in the last stage.

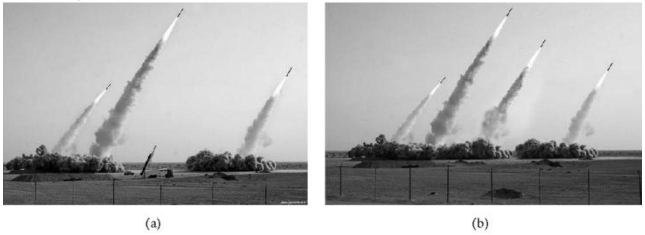


Fig.3-Copy-move forgery (a)Original image(b)Tampered image

In image splicing, one or more image fragments in an image is replaced by image fragments from some other image. They can be classified as region-based and boundary-based techniques.

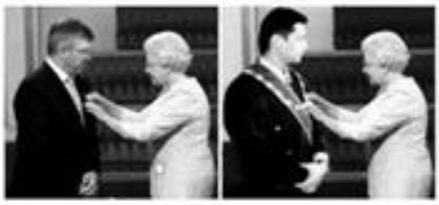


Fig.4- shows how an image can be easily forged where Wong Su En from DAP-China forged a photograph receiving a knighthood from Queen Elizabeth-II

The following section gives a brief overview on various copy-move forgery and splicing techniques. Many of the copy-move forgery techniques were based on block matching of image pixels directly, and are not well executed at the presence of geometrical or illumination deformations. Pan and Lyu [17] propose a robust method that does not deal with geometrical and illumination distortions, that starts with the estimation of transform between matched scale invariant feature transform(SIFT) keypoints . Thereafter discounting the estimated transforms,

all pixels within the duplicated regions are perceived. But it shows poor performance on detecting small duplicate regions.

Due to the problems in keypoint detection Cozzolino et al [18] suggests a method using rotational invariant features. To upgrade the performance, a modified version of Patchmatch algorithm and dense linear fitting for post-processing is used. This helps to achieve robustness with respect to rotation and scaling.

In [19] the technique deals with both splicing and copy-move detection depends on deep convolutional neural network. This method works on two stages. The first stage is feature learning in which a CNN model is pretrained, from the training images based on the patch specimens. This improves the generalization ability and accelerates the convergence of the network. The second stage is feature extraction where the features are extracted from an image with the pre-trained CNN . The resultant image undergoes compression by region pooling, a method for feature fusion. In order to check whether the image is authentic or forged, based on the resulting feature representation a SVM classifier is trained for binary classification.

Bahrami et al.[20] suggested a method for blurred image splicing detection and localization. It discriminates blurring due to out-of-focus and motion. The input tampered image is partitioned into blocks based on local blur type features and then they are classified into various blur types. Finally an energy based method is applied for the precise splicing localization. The drawback of this method is that it focuses only on blurred image. An interest point detector is proposed in [21], which utilizes the positive elements of both block-based and keypoint techniques. Based on distinctiveness metric the detected keypoints can cover the whole image, even in low contrast regions. By the help of a new filtering algorithm, falsely matched regions are avoided. Along with the keypoints density, the whole procedure is iterated. On each attempt, the interest points focus more crucially on sceptical regions, using the obtained information from the foregoing iterations.

C.FUSION METHODS

Initially the researches focus only on any one of the tampering problem in an image and finds a solution only for that problem. But, a tampered image may be produced with a number of tampering techniques. So a single solution is not sufficient to find out all the tampered regions. So now research work is mainly focused on fusion techniques, in which a number of tampering detection methods are fused together to obtain better results.

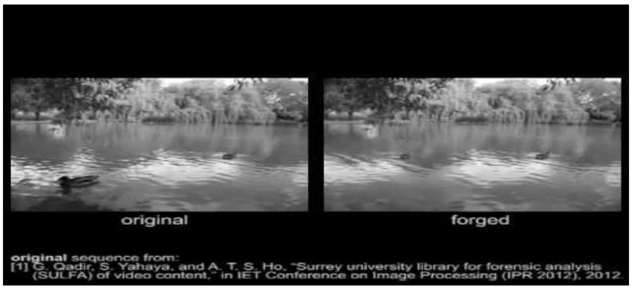
Even if we have lot of tampering detection and localization techniques, they work for any one of the tampering detection techniques or uses different datasets. So fusion and comparison of this techniques were difficult. Initilally it was the fusion of results, of several forensic detectors after analyzing the image. [22] a fuzzy theory and dempster shafer theory [23] approaches dealt with JPEG compression artifacts.[24] dealt with some universal features. An IFS-TC challenge was established in 2013 by the IEEE Information Forensics and Security Technical Committee. It has two stages. The initial stage was detection of forgery, in which Cozzolino et al [25] obtained the best results with score 0.9421.The second stage dealt with forgery localization, that requires analysis in the pixel level, not in the image level.

The winner of this challenge was [26] with a F1-score of 0.4072 and later by further modification [27] with an F1-score of 0.4533.Both this methods is a fusion of three approaches, and were using binary maps for tampering localization. The former technique dealt with the fusion of the results of Photo Response Non Uniformity (for source device identification),block matching (PatchMatch algorithm) and local descriptors(sliding window and SVM classifiers).The only difference in the later approach is the third detector ,a near duplicate detection based approach exploiting the image phylogeny.

In [28] Li et al make use of statistical feature and copy move forgery approach .Here, instead of using binary maps, they used tampering possibility maps which consists of more intermediate information's that is helpful to find out whether an image is fake or pristine. They got the F1-score as 0.4925.The forgery localization approach in [29] claims with the highest F1-score other than [26]-[28], which focuses only on a single clue, ie. image splicing. In this method, the Multi-Scale Convolutional Neural Network for patches that are in color of divergent scales are planned and trained as forgery detectors.

D.VIDEO TAMPERING

Due to the development of multimedia services, different authentication techniques are required to prove the originality and integrity of multimedia data. But, most of these authentication techniques focus only on digital images. When used in lawsuits, video sequences often provide robust forensic proofs than still images. Video tampering [30] is the process of altering the video content by inserting or deleting an object or frame, to change the meaning carry out by the video. Video tampering become a very simple endeavor by the help of video acquisition devices and video editing software tools. The attacker may use the source region from the source video or from a distinct video. Some video tampering detection techniques, deals with detection of insertion or removal of objects, while some techniques deals with the frame-based video tampering detection [32] and [33].



original sequence from:
[1] G. Qadir, S. Yahaya, and A. T. S. Ho, "Surrey university library for forensic analysis (SULFA) of video content," in IET Conference on Image Processing (IPR 2012), 2012

Fig.5-Video Tampering by deletion

In [31] the forged regions are located using correlation of noise residue. Frame-based tampering are usually subjected to double MPEG compression.[32] and [33], uses frame based video tampering

detection methods, the former method detects the forging depends on the power features of high frequency area in the forged video. It can identify tampering of frames in the MPEG-2 streams. The detection technique in [33] is MCEA based passive forensics technique and uses the MCEA distinction between adjoining frames. The final decision is taken after observing the formation of peaks in fourier transform after double MPEG compression. This approach identifies the insertion/deletion of frames. The approach in [34] focuses on the evidences left out by the attackers while tampering a video sequence. Here an unsupervised approach in the spatio-temporal domain is proposed to reveal video forgery localization which is robust to compression.

III. RESULT ANALYSIS

The previous section discusses on various image and video tampering detection techniques. The rest of the section dealt with the comparison of different approaches in each type of tampering detection methods. Digital watermarking is done by hiding some additional information in the image which helps to reveal the tampering in an image and is classified into fragile, semi-fragile and robust watermarking. But it is not a popular technique, since it requires some pre-processing even though it helps to manage the authenticity and integrity of an image.Tab.I shows a comparison table denoting the tamper rate, peak signal to noise ratio(PSNR) and the various attacks each method can handle.

Tab.I-Comparison table denoting different digital watermarking techniques

Methods	Tamper Rate (Rt)	PSNR(dB)	Deals on Attacks
12	44.24	12.42	Collage attacks Content tampering attack
13	35.77	15.9	Parity error Intensity relationship error
14	28.09	23.2	Cropping attacks Covering attacks Removing attacks Replacing attacks
16	27.12	32.05	Random paint-based attacks Stirmark-based attacks

Copy-move forgery and splicing techniques are passive tampering technique by copying and pasting image regions from related or unrelated digital images. Tab.II gives a general overview on the datasets and limitations of some of the copy-move and splicing techniques.

Tab.II-Comparison table denoting various copy-move and splicing techniques

Ref. No.	Methodology	Dataset	Disadvantages
17	SIFT keypoint (Copy-Move)	Self Constructed	• Cannot find genuine keypoints in areas with minimal visual elements. • Compact regions have insufficient keypoints , they are also difficult to identify. • Images that have inherently uniform areas cannot be differentiated
18	PatchMatch (Copy-Move)	FAU GRIP	• Higher processing time • Not robust against resizing
19	Deep Convolutional Neural Network (Copy-Move and Splicing)	CASIA v1.0 CASIA v2.0 Columbia gray DVMM	• Computational Complexity
20	Block-based blur type features (Blurred Image Splicing)	Self Constructed P1,P2,P3 Flicker website images	• Applied only on Blurred images • Do not work well, in the presence of both motion and out-of -focus blur.
21	Interest point detector (Copy-Move)	IMB SBU-CM16	• Not dealt with resizing attack

The fusion techniques will perform both tampering detection and localization by the fusion of various approaches. In order to obtain a standardized technique IEEE IFS-TC has organized a challenge using the given detection. Initial phase was for tampering detection and obtained a best score of 0.9421[25].Next phase was for tampering localization, for which a satisfactory results was not obtained and researches is going on in this field. The obtained results for the tested images ([26]-[29]) are proposed to the assessment system of the challenge for a fair comparison. The forgery localization performance is assessed with the F1-score based on the rules of the challenge,

$$F1=2*\frac{PR*RC}{PR+RC} \quad \text{—— Eqn.3.1}$$

where PR (precision) and RC (recall) respectively.

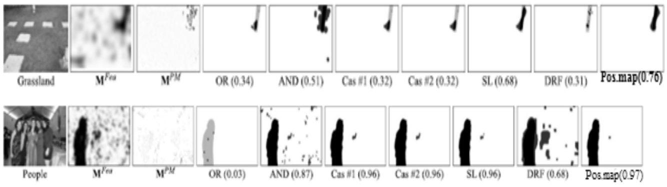


Fig.6:-F1-Scores of various fusion techniques

Tab.III-F1-Scores for methods based on statistical features, copy-move detection and fusion of PRNU, statistical and copy-move techniques

Ref.No	LD	PM	Fusion
26	0.1115	0.3425	0.4072
27	0.1737	0.2784	0.4533
28	0.3458	0.3845	0.4925

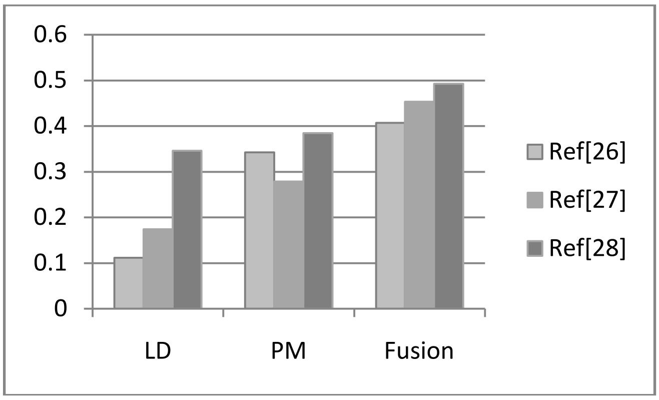


Fig.7:-Graph drawn based on the F1-Scores obtained on various techniques.

The F1-scores obtained are only less than 0.5. The results of various techniques has obtained only an average result. The above results shows that there is still scope on this research field.

IV. CONCLUSION

The authenticity and integrity of digital information has to be maintained, since these data may be used as evidence in investigations, military applications. The digital data may get tampered and with or without knowing ,people may use these tampered data which may lead to societal as well as political problems. So, before using the digital contents we must ensure that they are pristine. Researches were going on in the digital forensic field, for the detection and localization of tampered images and videos. Here, we made on a study on some of the widely used detection and localization techniques.

REFERENCES

1. Mathew C.Stamm,Min Wu,K.J.Ray Liu,"Information Forensics :An Overview of the First Decade",IEEE Access,vol.1,pp.167-200,May 2013.
2. H.Li,W.Luo,X.Qiu,J.Huang,"Image forgery loclalization via integrating tampering possibility maps,"IEEE Trans.Inf.ForensicsSecurity,vol.12,no.5,pp. 1240-1252,May 2017.
3. Warif N. B. A., Wahab A. W. A., Idris M. Y. I., Ramli R., Salleh R., Shamshirband S. and Choo K. K. R,"Copy-move forgery detection: Survey ,challenges and future directions",J.NetworkComp.Apps.,vol.75,,pp.259-278,Nov.2016.
4. O. Tayan, M. N. Kabir, and Y. M. Alginahi, ‘‘A hybrid digital-signature and zero-watermarking approach for authentication and protection of sensitive electronic documents,’’ Sci. World J., vol. 2014, Aug. 2014, Art. no. 514652
5. A. Tareef, A. Al-Ani, H. Nguyen, and Y. Y. Chung, ‘‘A novel tamper detection-recovery and watermarking system for medical image authentication and EPR hiding,’’ in Proc. 36th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc., Chicago, IL, USA, Aug. 2014, pp. 5554–5557
6. S. Walton, “Image authentication for a slippery new age,” Dr. Dobb’s J., vol. 20, pp. 18–26, Apr. 1995.
7. M. Schneider and S.-F. Chang, “A robust content based digital signature for image authentication,” in Proc. IEEE Int. Conf. Image Processing, 1996, vol. 3, pp. 227–230.
8. R. B. Wolfgang and E. J. Delp, “A watermark for digital images,” in Proc. IEEE Int. Conf. Image Processing, 1996, vol. 3, pp. 219–222.
9. M. M. Yeung and F. Mintzer, “An invisible watermarking technique for image verification,” in Proc. IEEE Int. Conf. Image Processing, 1997, vol. 2, pp. 680–683.
10. H. He, F. Chen, H.-M. Tai, T. Kalker, and J. Zhang, ‘‘Performance analysis of a block-neighborhood-based self-recovery fragile watermarking scheme,’’ IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 185–196, Feb. 2012.
11. B. Patra and J. C. Patra, ‘‘CRT-based fragile self-recovery watermarking scheme for image authentication and recovery,’’ in Proc. Int. Symp. Intell. Signal Process. Commun. Syst. (ISPACS), Taipei, Taiwan, Nov. 2012, pp. 430–435.
12. H.-J. He, J. S. Zhang, and F. Chen, ‘‘Adjacent-block based statistical detection method for self-embedding watermarking techniques,’’ Signal Process., vol. 89, pp. 1557–1566, Aug. 2009.
13. P. L. Lin, C.-K. Hsieh, and P.-W. Huang, ‘‘A hierarchical digital watermarking method for image tamper detection and recovery,’’ Pattern Recognit., vol. 38, no. 12, pp. 2519–2529, 2005.
14. T-Y. Lee and S. D. Lin, ‘‘Dual watermark for image tamper detection and recovery,’’ Pattern Recognit., vol. 41, no. 11, pp. 3497–3506, 2008.
15. Abdulaziz Shehab , Mohamed Elhoseny , Khan Muhammad , Arun Kumar Sangaiah , Po Yang , Haojun Huang , And Guolin Hou,"Secure and Robust Fragile watermarking scheme for medical images",IEEE Access,vol.6,pp.10269-10278,Feb 2018.
16. Lamri Laquamer and Omar Tayan," Performance Evaluation of a Document Image watermarking approach with enhanced tamper localization and recovery", IEEE Access,vol.6,pp.26144-26166,Feb 2018.
17. Xunyu Pan and Siwei Lyu," Region Duplication Detection Using Image Feature Matching", IEEE Transactions On Information Forensics And Security, Vol. 5, No. 4, Dec 2010
18. Davide Cozzolino, Giovanni Poggi and Luisa Verdoliva," Efficient dense-field copy-move forgery detection", IEEE Transactions On Information Forensics And Security, Vol. 10,Iss. 11,pp. 2284 - 2297 Jul 2015.
19. Yuan Rao, Jiangqun Ni, GuangZhou and GuangDong"A Deep Learning Approach to Detection of Splicing and Copy-Move Forgeries in Images," IEEE International Workshop on Information Forensics and Security (WIFS)2016.
20. Khosro Bahrami, Alex C. Kot, Leida Li and Haoliang Li," Blurred Image Splicing Localization byExposing Blur Type Inconsistency", IEEE Transactions On Information Forensics And Security, Vol. 10, No.5, May 2015.
21. Mohsen Zandi, Ahmad Mahmoudi-Aznaveh, and Alireza Talebpour,"Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector,"IEEE Transactions on Information Forensics and Security, Vol.11, Iss. 11, Nov. 2016.
22. M. Barni and A. Costanzo, “A fuzzy approach to deal with uncertainty in image forensics,” Image Commun., vol. 27, no. 9, pp. 998–1010, 2012.
23. M. Fontani, T. Bianchi, A. De Rosa, A. Piva, and M. Barni, “A framework for decision fusion in image forensics based on Dempster–Shafer theory of evidence,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 4,pp. 593–607, Apr. 2013.
24. X. Qiu, H. Li, W. Luo, and J. Huang, “A universal image forensic strategy based on steganalytic model,” in Proc. 2nd ACM Workshop Inf. Hiding Multimedia Secur., New York, NY, USA, 2014, pp. 165–170.
25. D. Cozzolino, D. Gragnaniello, and L. Verdoliva, “Image forgery detection through residual-based local descriptors and block-matching,” in Proc. IEEE Int. Conf. Image Process., Oct. 2014, pp. 5297–5301.
26. D. Cozzolino, D. Gragnaniello, and L. Verdoliva, “Image forgery localization through the fusion of camera-based, feature-based and pixel based techniques,” in , Oct. 2014, pp. 5302–5306.
27. L. Gaborini, P. Bestagini, S. Milani, M. Tagliasacchi, and S. Tubaro, “Multi-clue image tampering localization,” in Proc. IEEE Int.Workshop Inf. Forensics Secur., Dec. 2014, pp. 125–130.
28. Haodong Li, Weiqi Luo, Xiaoqing Qiu, and Jiwu Huang, “Image forgery localization via integrating tampering possibility maps,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 5, pp. 1240– 1252, 2017.
29. Yaqi Liu, Qingxiao Guan, Xianfeng Zhao, and Yun Cao," Image Forgery Localization Based On Multi-Scale Convolutional Neural Networks",in Proc.ACM Workshop on Info .Hiding & Multimedia Security., Jun. 2017.
30. K.Sitara,B.M.Mehtre,"Digital Video Tampering Detection:An Overview of passive techniques",in J.Digital Investigation,Vol.18,pp.8-22,Sept.2016.
31. Chih-Chung Hsu,Tzu-Yi Hung,Chia Wen Lin and Chiou-Ting Hsu," Video Forgery Detection using correlation of noise residue", in IEEE workshop on multimedia signal processing, Nov 2008.
32. Yuting Su,Weizhi Nie,Chengqian Zhang,"A frame tampering detection algorithm for MPEG videos",in IEEE Joint Int. Information Technology and Artificial Intelligence Conference,Sept.2011.
33. Qiong Dong,Gaobo,Yang,Ningbo Zhu,"A MCEA based passive forensics scheme for detecting frame-based video tampering",in J.Digital Investigation,Vol.9,Iss.2,pp.151-159,Nov.2012.

34. Paolo Bestagini, Simone Milani, Marco Tagliasacchi, Stefano Tubaro,"Local tampering detection in video sequences",in IEEE Int.Workshop on Multimedia Signal Processing,Nov.2013.
35. Priyanka Singh,Balasubramanian Raman,Nishant Agarwal," Towards encrypted video tampering detection and localization based on POB number system over cloud", IEEE Transactions On Circuits and Systems for Video Technology, Jun. 2017 .
36. Vahideh Amanipour and Shahrokh Ghaemmagham," Video Tampering detection & Content Reconstruction via Self Embedding", IEEE Transactions On Instrumentation and measurement, Vol.67,No.3,Mar. 2018 .

AUTHORS PROFILE

Silpa Joseph received the B.E. degree from Madras university, Pallavan College Of Engg., Kanchipuram in 2004, M.E. degree from Karunya university, Coimbatore in 2007.She has 12 years of teaching experience. She is currently working as an Associate Professor, CSE Dept. at Viswajyothi College of Engg. and Technology, Vazhakulam , Kerala. Her current research interests include Image and Signal Processing, Cryptography and Network Security and Image Forensics. She has 5 publications in national and international journals and conferences.

S Palanikumar received the B.E. degree from Manonmaniam university, Government College Of Engg.,Tirunelveli in 1999, M.E. degree from Bharathiar university, Government College Of Engg., Coimbatore in 2001 and the Ph.D. degree from Anna university, Noorul Islam College of Engineering, Kumaracoil in 2013. He has 1.5 year of Industry experience and 16 years of teaching experience. He is currently an Associate Professor , IT Dept. at Noorul Islam Centre for Higher Education, Kumaracoil. His current research interests include Image and Signal Processing, Software Engineering, Biometrics and Embedded and Computer communication Systems. He has more than 25 publications in national and international journals and conferences.