International Journal of Electrical and Computer Engineering (IJECE)
Vol. 7, No. 6, December 2017, pp. 3558~3569
ISSN: 2088-8708, DOI: 10.11591/ijece.v7i6.pp3558-3569

Reviewing the Effectivity Factor in Existing Techniques of Image Forensics

Shashidhar TM[1], Dr. KB Ramesh[2]
[1]Visvesvaraya Technological University, Belagavi, Karnataka, India
[2]Dept. of Electronics and Instrumentation Engg, RV College of Engg, Bengaluru, Karnataka, India

Article Info

Article history:

Received Mar 14, 2017
Revised Jun 23, 2017
Accepted Jul 15, 2017

Keyword:

Image forensic
Anti-forensic
Image forgery
Copy-move attack
Image splicing
Image attacks

ABSTRACT

Studies towards image forensics are about a decade old and various forms of research techniques have been presented till date towards image forgery detection. Majority of the existing techniques deals with identification of tampered regions using different forms of research methodologies. However, it is still an open-end question about the effectiveness of existing image forgery detection techniques as there is no reported benchmarked outcome till date about it. Therefore, the present manuscript discusses about the most frequently addressed image attacks e.g. image splicing and copy-move attack and elaborates the existing techniques presented by research community to resist it. The paper also contributes to explore the direction of present research trend with respect to tool adoption, database adoption, and technique adoption, and frequently used attack scenario. Finally, significant open research gap are explored after reviewing effectiveness of existing techniques.

Corresponding Author:

Shashidhar T M,
Research Scholar,
Visvesvaraya Technological University Belagavi, Karnataka, India
Email: shashilara@gmail.com

1. INTRODUCTION

Image plays a very big role in when it comes to information propagation. This is the easiest, fastest, and most effective way to transmit information over the varied communication channel [1]. There are various forms of application e.g. matrimonial application, social networking application, as well as business based application, where value of image is highly emphasized. The user of such application undergoes a collateral loss associated with defamation if such images are maliciously tampered. At present, there are more than thousands of free image editing applications that can be used for this purpose [2]. This software have the capability of performing photorealistic graphics on computer which makes the viewer so much confused about real and forged image [3]. As a result of this the numbers of doctored images are increasing at a faster pace in digital era that potentially diminishes the trust level. Forensic expert deals with such complexities to explore the original and dubious images using their expertism as well as with different sophisticated tools [4]. However, the task of such exploration process is never an easy job especially if such image-based attacks are superiorly done with higher degree of imperceptibility. There has been a significant research work being carried out towards anti-forensic techniques [5] [6] in order to address this problem. The existing techniques are broadly classified as active-based approach and passive-based approach in image forensics [7]. Basically, the active-based approach is mainly a technique that emphasizes more on the trust factor of the image that enable certain amount of security operation to be carried out over digital image capturing device. The passive-based approach is mainly focused on performing an evaluation over the digital image and nothing else. The research work carried out towards image forensics using active approaches mainly depends upon the secured and trusted image capturing device that incorporates two secured tokens i.e. digital watermark

and digital signature [8]. This incorporation of secured token is carried out at the time of image acquisition. Therefore, if this secured image undergoes any form of illegitimate changes than the digital signature/watermark will never match. Thereby the detection of the image forgery is carried out. However, such techniques are also shrouded with some significant pitfalls. Majority of the commercial camera doesn't come up with such features and watermarked image is never demanded by any user from application usage viewpoint. There are certain brands e.g. Kodak and Epson that performs digital watermarking; however; such cameras are never in demand from normal usage viewpoint. Such camera has a digital chip that performs either digital watermarking or digital signature incorporation. It then performs securing the captured image prior to storage in its memory units. In order to ensure the prevalent usage of such digital camera, it is required that the manufacturer of such camera will need to adhere it to a uniform security protocol. This is quite far from reality in order to be accomplished for billions of trillions of camera users worldwide. Therefore, such forms of research techniques sound good, but they are highly unpractical in real-life implementation.

Therefore, this paper reviews the existing research techniques towards exploring the level of effectiveness of existing contribution towards image forensics. The secondary aim of this paper is also to derive the research trend as well as significant research gap that could be addressed in upcoming research work. Section 2 discusses about essentials of image attacks that has been frequently found in existing literatures followed by discussion of research trends in Section 3. Existing research techniques with their limitation are elaborated in Section 4 followed by brief discussion of explored research gap in Section 5. Finally Section 6 makes some concluding remarks.

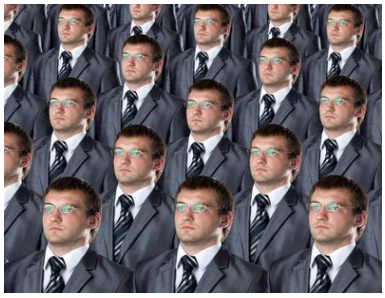
2. ESSENTIALS OF IMAGE ATTACKS

This section presents a brief discussion of different forms of image attack reported in existing research implementation.

2.1. Cloning-Based Attack

Image cloning is the most frequently used image-based attack which performs the mechanism of copying the image and pasting it elsewhere in order to hide certain object. A simple image cloning is quite easily understood of its artifacts (Figure 1 (a)); however, a sophisticated image cloning is quite hard to be identified about its original source (Figure 1 (b)). One of the challenging tasks in these forms of attack is to explore the exact area of the forged image. There are certain existing techniques e.g. [9, [10], [11], [12], [13], etc that has attempted to address this problem of image attack. Such techniques are found mainly to use transform based techniques as well as principle component analysis in order to control the computational complexity.

(a) Simple Cloning



(b) Sophisticated Cloning

Figure 1. Image Cloning Attack

2.2. Image Splicing Attack

Image splicing attack results in generation of a new forged image by fusing two or more different images. A sophisticated image splicing results in the generation of the spliced image that is quite difficult to be traced in case the border of the spliced image is carefully edited. The mechanism of image slicing can be carried out using normal photoshop software or other easily available photo-editing tools. Although, image splicing also looks quite similar to photo montages, but there are some significant differences. Image splicing is not reported to be carried out with post processing but photo. This feature is normally applied while designing anti-forensics. Figure 2 showcases the formation of spliced image [14].

(a) Image-1 (b) Image-2 (c) Spliced Image from Image-1 & Image-2

Figure 2. Image Splicing Attack

2.3. Copy-Move Attack

This is one of the most frequently used image attacks studied in the area of image forensics. In such form of image forgery, normally a segment of an image or an object is copied and then pasted in different form of image such that the newly inserted image (or an object) looks like a genuine part of it. The primary target of such attacks is to hide certain sensitive information in the original image with counterfeit object in order to deceive the user. Figure 3 shows the simple example of copy-move attack where the first one show a presence of two vehicle while one of the vehicle is deliberately found missing in the second image [15].

Figure 3. Copy-Move Attacks

2.4. Image Retouching

Image retouching is another frequently used image forgery techniques. Although, image retouching is normally adopted for performing enhancement of the image feature, but it could be lethally used for the malicious purpose. The process of image retouching doesn't completely alter the image to a large extent; however, a smaller scale of editing is normally carried out in order to either minimize or maximize certain potential feature of an image [16].

Figure 4. Image Retouching

2.5. Image Resampling

Image resampling is the process of altering the dimension of the input image for malicious purpose. There are certain operations e.g. stretching the segments of an image or resizing the image in order to carry out image forgery. Resampling operation is required to be carried out over the original image over a novel sampling lattice thereby incorporating specific periodic correlation among all the adjacent pixels. Although, such correlation have a quite less probability to occur; however, their existence could adversely affect such form of image forgery. Figure 5 showcase the typical example of image resampling where the first figure shows the image with 72 DPI while the second one shows the magnified version of the same image in 300 DPI [17].

Figure 5. Image Resampling

There are various forms of image-based attacks evolving with the surfacing of the new forms of image editing tools. Figure 6 highlights the taxonomies of image attacks on the basis of frequent observation from the existing studies. Essentially, there are three forms of attacks i.e. geometric-based (applies operations e.g. rotation, zoom, cropping, shearing), enhancement-based (applies operations e.g. Histogram equalization, color modification, contrast adjustment, filtering), and content modification (applies operations e.g. copy-move, cut and paste, seam carving). Conventionally, there are two different technique of performing detection of image-based attacks. i.e. i) signal processing approaches and ii) Geometry-based approaches. The first process uses signal processing-based tools as well as statistical-based tools in order to identify the forged image. On the other hand, geometric based mechanism addresses the image forging techniques using rotation, zoom, cropping, and searing. There is a significant level of benefits pertaining to such approaches. Geometric-based approach is free from any form of low-level features associated with an image. Such approaches are also found to be quite potential towards various forms of operation e.g. filtering, compression, etc. Majority of the existing techniques towards image forgery is on the basis of complexities associated with image-based attacks to be consistent over the geometric viewpoint. This will also mean that majority of the existing image-based forgeries are connected with residuals of artifacts where some of them are perceptible in naked eye and some are not. However, there are higher probabilities of resurfacing the consistencies during very common and simple form of attack i.e. cut and paste attacks. On the other hand, copy and move attack is one of the most challenging forms of the image-based attack to be identified using simple tools even. Another interesting fact about such image forgeries is that all of them are human assisted based attacks and hence there are many variations of it. Out of all variations of attacks, majority of them are not even reported in existing research work. Another significant problem is existing anti-forensic techniques are incapable of even assessing the level of threat for massive number of images. Normally such forms of images reside in publically available image dataset, which can cause a collateral damage.

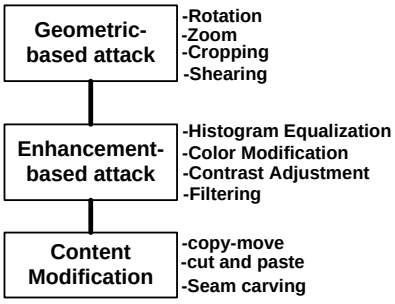


Figure 6. Taxonomies of Image Attacks

The existing techniques of image-forgery detection are essentially found classified into active-based approach and passive based approach. The active-based approach makes use of pre-processing with an aid of digital signature/watermark [18]. Although, active approaches of image forgery detection is mainly preferred for checking the integrity of the suspected image but such options and features for supportability is not present in existing imaging devices. On the other hand, the passive-based approach is mainly focused on using multiple techniques in order to perform identification of image-attacks [19]. Different forms of statistical attributes as well as semantic information are derived from the raw image itself. The exact identification of tampering is carried out on the basis of the statistical image features. It is again classified into forgery-type dependent and forgery-type independent. Figure 7 showcases the taxonomies of anti-forensic techniques found to be exercised in existing literatures.

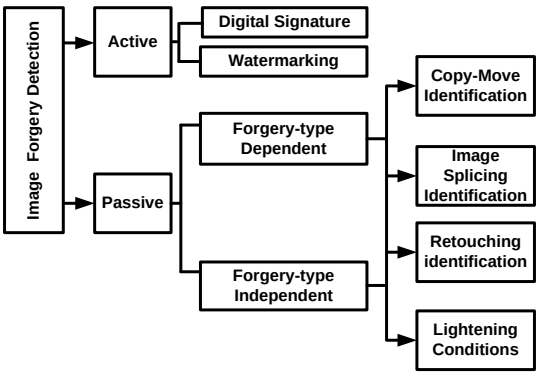


Figure 7. Taxonomies of Anti-Forensic Techniques

3. RESEARCH TREND

It is quite a challenging task to identify the research trends towards digital image forensic techniques. There are good numbers of research papers being published in the direction of the image forgery detection techniques.

3.1. Trend towards Tool Adoption

At present, there are various image editing tools that can easily use for carrying out image forgery. Some of the potential tools are i) Adobe Lightroom, ii) Adobe Photoshop, iii) GIMP, iv) Affinity Photo, v) Acorn, etc [20]. The conventional tools discussed for digital forensics are shown in Figure 8. However, there is a gap between reality and research work. We find that research papers doesn't directly discuss much about acquisition or generation of forged image from this frequently used image editing tools. Apart from this, there are also many image editing apps in android phones e.g. i) Instagram, ii) Snapseed, iii) Pixlr, iv) PicsArt, v) Cymera, vi) Aviary, etc [21]. We don't find research work that considers degradation of image due to such applications.

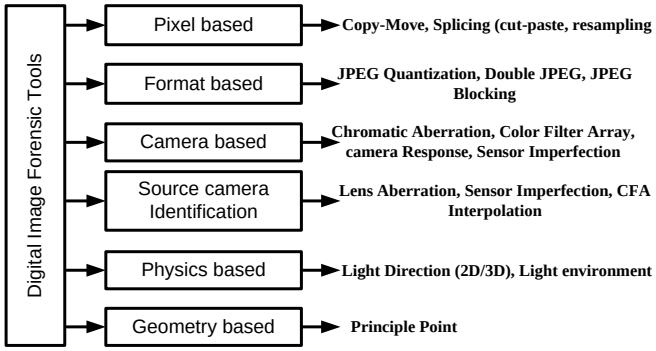


Figure 8. Different Forms of Digital Image Forensic Tools

3.2. Trend towards Database Adoption

The different forms of the dataset found to be adopted by various researchers are i) Image Manipulation Dataset [22], ii) Direct and Sparse Odometry (DSO) dataset [23], iii) CASIA tampered image dataset [24], iv) BOSSBase dataset [25], v) UCID dataset [26], vi) MICC-F600 dataset [27], etc. These datasets are highly standardized and is frequently used for the study of image forensics. Although, testing with dataset offer reliability to outcome, but it doesn't ensure similar performance in real-time image.

3.3. Trend towards Techniques

Different forms of techniques have been reported till date pertaining to identification of forged image. We find presence of certain techniques e.g. JPEG Compression, Support Vector Machine for optimizing the classification process in detection performance, searching-based techniques, sliding window, Gaussian Model, Expectation-Maximization algorithm, injection of key-points, color filter array based techniques. However, all the techniques are not meant for addressing similar problem of identification. These techniques are found to have potential to address decision making problem, identification of key points, illumination, along with common goal of identification of tampered region for the given input image.

3.4. Trends towards Attack Specifications

The prior sections have elaborated varied forms of image forgeries as well as tools used to identify them. According to our investigation, we find that majority of the existing research work is carried out towards image splicing attack followed by copy-move attack. Although, there are some extent of work being carried out towards image retouching attack, but it is comparatively low compared to splicing and copy-move attack. Figure 9 shows the statistics of existing research work published on various reputed research-based journals till date.

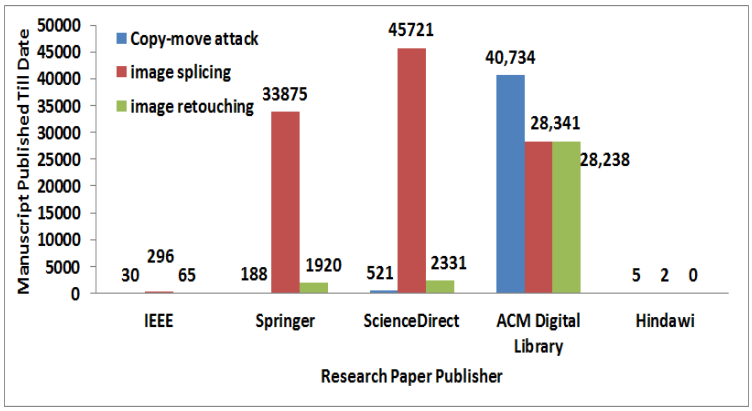


Figure 9. Research Trends on Image Attacks

4. EXISTING TECHNIQUES

This section discusses about some of the recent research techniques towards mitigating different forms of image attacks in-terms of image forgeries. This section discusses only the recent and most frequently used techniques of research published between the years 2010-2016. Zandi et al. [28] have presented a technique that can identify the position within an image inflicted by copy-move attack. The technique uses key-point as well as block-based in order to introduce a detection method of interest point. Finally, the technique also search for complex region that is found mismatched during the identification of attacks. Carvalho et al. [29] have discussed a method for identification of regions that is illegitimately transformed. The authors have used statistical approach using visual descriptors. The study outcome was assessed for its accuracy of detection using KNN algorithm. The technique presented by Korus and Huang [30] have addressed the problem of localizing tampered region of an image using sliding-window based approach as well as random walk approach. A tampered image is considered as an input that is subjected to sliding window for analysis in order to generate a response map. This map was further analyzed for extracting region importance followed by visual organization. Finally, a thresholding is applied to confirm

the localized area. Similar author have also present similar technique of identification of forged region of an image using unsupervised multi-scale approach [31].

Pun et al. [32] presents a discussion of tamper localization technique using geometric transformation technique. The technique initially applies adaptive segmentation process followed by construction of image hash in order to generate forensic hash. The technique also emphasizes on detection of image alignment and also uses multi-region matching. The study outcome shows good accuracy, precision, and recall performance as well as f-measure. Study towards tampered region localization is carried out in a different fashion as seen in the work of Thai et al. [33]. The authors have presented a technique for computing the steps of quantization of the image that has been priory compressed using JPEG. A mathematical framework is presented in this technique along with construction of quantization table. Connoter et al. [34] have introduced a technique that is capable of identifying all the forgeries being inflicted over the image. The authors have implemented linear filtering mechanism along with conventional JPEG compression. Peng et al. [35] have presented a technique that focuses on illumination factor as well as occlusion geometry along with significant textural information. The authors have presented a reflection model for untextured as well as non-convex surface. Cozzolino et al. [36] have addressed the problem of copy-mode attack by presenting a technique that uses rotation-invariant charecteristics. The author has implemented a nearest-neighbor search technique for exploring the dense fields for a given counterfeited image. The work carried out by Li et al. [37] has associated image compression with image forensics.

The technique assists in hiding the artifacts of lossy compression during coding process. Dither noise is added alongside with prediction error for developing predictive approach. Rosa et al. [38] have presented a forensic approach using statistical strategy of second order that is computed from the co-occurances matrix. The study outcome was assessed using confusion matrix over gamma correction and histogram stretching mechanism over original image, enhanced image, and remapped image. Dam et al. [39] have addressed the problem associated with face reconstruction in image forensics. The technique uses Lambertain reflectance model for construction the facial image in the form of three dimensions. The study outcome is found with 90% of accuracy. Fan et al. [40] have discussed the usage of median filter towards anti-forensics. A deconvolution framework is presented along with optimization approach. A distributive framework using Gaussian approach was used for normalizing the derivative values of the pixels. Li et al. [41] have presented a simple identification mechanism for copy-move attack using segmentation methodology. The technique is also followed by expectation maximization approach. Cao et al. [42] have presented a technique that performs detected of the forged image based on the contrastive factor of a corrupt JPEG image. A clustering technique is applied for identified blocks being manipulated for evaluating its respective consistency. Costanzo et al. [43] have addressed the security problems associated with removal of SIFT key-points in connection with copy-move forgery detection.

The technique mainly focuses around identification of varied form of anomalies in the key-point distribution. Fontani et al. [44] have used Dempster-Shafer for undertaking a precise decision in order to identify the location corrupted by any significant image attacks. A mathematical modeling is presented along with combination rule in order to conclude about final decision. Li et al. [45] have addressed the problems related to the incapability of color filter array to deal with certain specific kind of non-uniformity noise. This property is sometime used for malicious purpose in image forgery. Therefore, this work presents a technique of decoupling noise from color that can sufficiently mitigate the propagation of interpolation noise. Sun et al. [46] have presented a steganography-based model in order to secure information within an image. The technique uses differences over the pixel values in order to find the location. Luo et al. [47] have presented a technique for performing analysis of JPEG error that includes various significant steps e.g. quantization followed by rounding and truncation errors. The technique also introduces a scheme for identifying a bitmap image that has been prior compressed using JPEG. Therefore, it can be seen that there are various forms of research-based techniques to resist the image-based attack by introducing various anti-forensics techniques with different forms of capabilities.

Table 1. Summary of Existing Techniques

Authors	Problem	Technique	Advantage	Limitation
Zandi et al. [28]	Copy-move attack	Detection of interest point Dataset: Image manipulation Dataset	-Simple Detection Technique -Faster Response Time	Not applicable for other forms of image-attacks
Carvalho et al. [29]	Impersonating image regions	Visual descriptors, statistical approach, K-Nearest neighborhood Dataset: DSO-I, DSI-I	-Higher accuracy	-leads to iterative approach. -computationally complex
Korus and	Detection of tampered	-Sliding window	-supports both double	-Only effective for splicing

Authors	Problem	Technique	Advantage	Limitation
Huang [30] [31]	region	-random walk -multi-scale Dataset: BOSS dataset	and single compression	attack.
Pun et al. [32]	Tampered region localization	-segmentation -image hash Dataset: CASIA	Good Precision over colored image	-involves computational cost
Thai et al. [33]	Tampered region localization	-quantization -Discrete Cosine Transform Dataset: BOSSBase	Good Accuracy	Involved computational cost
Connoter et al. [34]	Analyzing chains of operators. Recovery of original tampering operation	Linear Filtering JPEG Compression Support Vector Machine Dataset: UCID	99.6% accuracy	Highly dependent upon training operation.
Peng et al. [35]	Illumination	Relaxation of constant reflectance & convexity Dataset: Syn1, Syn2, YaleB, Multi-PIE, DSO-I	Good rate of detection	Involves computational complexity
Cozzolino et al. [36]	Copy-move attach	Searching using Nearest neighbor, rotation-invariant Dataset: GRIP database	Efficient computing	Less robust to geometric distortion and image resizing
Li et al. [37]	Anti-forensic (hiding artifacts of lossy compression)	Preserving prediction direction Dataset: UCID-v2 corpus	Higher success rate	-No comparative analysis -iterative process leading to storage complexity
Rosa et al. [38]	Statistical attack	Second order analysis Dataset: UCID-v2 corpus	Increased probability of detection	-iterative process leading to storage complexity
Dam et al. [39]	Face reconstruction	Lambertain Reflectance model Dataset: CMU multi-PIE,	Higher recognition rate	Testing over color images are not discussed
Fan et al. [40]	Artifact hiding	Median filter, Gaussian Model Dataset: UCID-v2 corpus	Good Accuracy, simple approach	Involves higher computational cost
Li et al. [41]	Copy-move attack	Expectation-Maximization, Segmentation Dataset: MICC-F600	Good Accuracy	Involves higher computational cost due to iterative process
Cao et al. [42]	Forged image to be detected using contrast	Artifacts of histogram, JPEG compression Dataset: BOSS Public dataset, UCID,	High performance	Doesn't addresses complexities associated with dataset
Costanzo et al. [43]	Identification of SIFT key-points	Key-point injection, region classification, Dataset: INRIA Holidays, UCID dataset.	Solves majority of key-point based problems	Outcomes not benchmarked
Fontani et al. [44]	Decision making	Dempster-Shafer Dataset: Unknown	Higher accuracy in decision making	Outcomes not benchmarked
Li et al. [45]	Non-uniformity noise, interpolation noise, image artifacts	Decoupling mechanism, Color Filter Array Dataset: Unknown	Independent of any prior information	Outcomes not benchmarked
Sun et al. [46]	Securing information	Steganography Dataset: normal images e.g. Lena, Barbara ,Baboon	Good retention of PSNR	Outcomes not benchmarked
Luo et al. [47]	Analysis of JPEG error	JPEG compression Dataset: Corel, NJIT, NRCS, UCID	Effective operation towards error analysis	Computational complexity is not addressed

5. RESEARCH GAP

The previous section has discussed about some of the related and significant research contributions towards addressing the problems associated with image forgery. Varied forms of algorithms and approaches has been utilized in the existing techniques, where of the algorithms are simpler to implement while some are quite sophisticated. Adoption of JPEG based approaches are more in abundant in the literature. A closer look will show the inefficiencies of quantization operation carried out using JPEG. It is because of the reason that modern image acquisition device performs JPEG compression on the image. Hence, performing any form of editing operation on the top of it will further aggravate the problems associated with JPEG compression. Equivalent issues can be also seen when chromatic aberration-based approaches have been considered in literatures. There is less number of research work that addresses the problems of evaluating chromatic aberration using only a less number of components with spatial frequency over the image blocks. Such techniques are absolutely found not capable to perform accurate image forgery detection over a larger region on the input image with uniform pixel density with less number of spatial frequencies. The forgery type

independent based approaches are also found with less effective work towards illumination factor. Such techniques are successful over exploring the tampered region with consistent illumination factor; however, in case of any sensitive operation in illumination, the system fails. Moreover, in presence of varied degree of occlusion, it is never possible to perform any form of forgery detection. Such approaches fail to perform forensic operation in presence of occlusion even if the environment is completely illuminated with different sources of light. These forms of techniques may be efficient when image forgery detection is carried out in controlled environment like inside the room.

However, such techniques are never proven to work on outside environment. The literatures have been also found to make use of camera response function and various other performance parameters that leads to minor errors in the outcomes. Adoption of such technique is still a question mark on JPEG standard. Such technique can never offer assurance to search for original camera utilized. Hence, it can be said that although there are massive number of literature being present in current times, but all of them are also accompanied by problems of smaller or bigger scale. After reviewing the research techniques as well as the outcomes of the existing system, it is strongly felt that there should be more strengthening the line of research direction towards exploring better image forgery detection mechanism. Some of the existing survey work carried out by Sharma et al. [48], Diane et al. [49], Quereshi et al. [50], and Poisel et al. [51] have also discussed about various significant research techniques. All the techniques have its own scope and limitation, which is quite natural but still there are certain open research issues that are yet not being considered in any of the research work till date associated with image forensics. This section will brief out such points to showcase the significant research gap:

5.1. Lack of Benchmarked Outcomes

There are more than thousands of research publications towards image forgery but we don't find any form of benchmarked outcome being adopted or discussed. The biggest challenge is that in the absence of benchmarked outcome, it is quite a difficult task to rate the effectiveness of any presented research work just on the basis of experimental data. The dataset Dresden Image dataset is reputed for its benchmarking capabilities [52], but quite a few of the existing research techniques have used them. Therefore, there is a need to evolve up with novel benchmarked outcomes to further gain a better reliability in outcomes.

5.2. Higher Dependence towards Dataset

Experimenting on the tampered image dataset is always a good and safe idea to cross check the outcomes of identification of image forgery. The biggest problem is such dataset are synthetically created along with pre-defined preprocessing operation already carried out before launching into public domain. It is still an open end questions about the sustainability of an existing algorithms of image forgery detection using dataset when swapped by real-time captures. It is because real-time captures will be required to undergo an unknown level of preprocessing depending upon the condition of captures [53]. Therefore, it is indefinite if the existing techniques do really have similar performance claims as there is no research work that has used both dataset and real-time captures to show robustness.

5.3. Low Focus on Algorithm Complexity

It can be thought that success rate of algorithm is superior if it can suitably and precisely capture the tampered regions. It will really doesn't matter much if such algorithm does so with bigger or lower resources cost. However, at present, many of the applications have started migrating to low-power communication devices where both power and other device-based resource do really matter. At present, none of the existing techniques have claimed to offer cost effective algorithm performance without any deviation to image forgery detection mechanism [54]. Hence, there is no balance between image forgery detection accuracy with algorithm complexity performance.

5.4. Adoption of Similar Forms of Attacks

We have discussed in this paper that majority of the existing research work is more oriented towards two forms of attacks either image splicing or copy-move attack. Hence, keeping the similar attack and working over the similar datasets of tampered image, the existing techniques have presented various forms of algorithm towards such attack. However, there are also other forms of attacks being possibly created by other un-discussed image editing tools that were never being considered [55]. For an example, image splicing operation created by two different image editing tools is very less likely to be identified with similar performance by one algorithm. Hence, exploration of new forms of attacks and consideration of more tools are required.

5.5. Non-equilibrium between Detection and Quality

Existing tools to perform image forgery detection applies different levels of algorithms over the input image. After a series of the algorithm implementation over an image, it is more likely that the input image has undergone significant processing that has all the possibility of degrading its quality. At present, we don't find much work in literature where the image quality is being emphasized to a larger extent. Ignoring the image quality will be quite detrimental if in future any iterative based algorithm is applied over larger epoch values [56]. Hence, blocking artifacts will autonomously re-appear to a smaller extent in such techniques. Usage of iterative algorithms may further worsen the situation of eliminating blocking artifacts. Hence, such problem of trade-off between forgery detection and image quality is still open ended.

6. CONCLUSION

This manuscript has briefly discussed about the fundamentals of image-forensics with special focus on exploring the effectiveness of existing techniques. The conventional technique of active and passive based techniques are now out-numbered with different other techniques that is discussed in this papers. We also discuss about the line of direction of existing research trends to find that still the popularity of addressing copy-move attack and image splicing attack is more within research community. The existing analysis of research techniques shows presence of both advantages and disadvantages. Finally, we discuss about the research gap which is found not to be addressed by existing researchers. Our future research direction will be towards addressing such open research issues. We will develop a novel framework for carrying out a mechanism for making it hard or near to impossible to retrieve information during an investigation of any image. Hence, it will be more focused on anti-forensic mechanism.

REFERENCES

[1] W. Chen, C. Castillo, L.V.S. Lakshmana, "Information and Influence Propagation in Social Networks", Morgan & Claypool Publishers, pp. 177, 2013.
[2] K-K.R. Choo, A. Dehghantanha, "Contemporary Digital Forensic Investigations of Cloud and Mobile Applications", Syngress, pp. 326, 2016.
[3] H.T. Sencar, N. Memon, "Digital Image Forensics: There is More to a Picture than Meets the Eye", Springer Science & Business Media, technology & Engineering, pp. 372, 2012.
[4] P. Sutthiwan, "Image Statistical Frameworks for Digital Image Forensics", New Jersey Institute of Technology, Department of Electrical and Computer Engineering, pp. 116, 2012.
[5] J. Spadea, "IOS Mobile Device Anti-forensics", Apple computer, pp. 80, 2012.
[6] M.P. Evison, R.W.V. Bruegge, "Computer-Aided Forensic Facial Comparison", CRC Paper, pp. 209, 2016.
[7] C-T. Li, "Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security", Idea Group Inc (IGI), pp. 345, 2013.
[8] K-Pour, Mehdi, "Encyclopedia of Information Science and Technology, Third Edition", IGI Global, Computers, pp. 10384, 2014.
[9] W. J.T. Mitchell, "Cloning Terror: The War of Images, 9/11 to the Present", University of Chicago Press, pp. 2009, 2011.
[10] B. Nikkel, "Practical Forensic Imaging: Securing Digital Evidence with Linux Tools", No Starch Press, pp. 320, 2016.
[11] J. Sammons, "The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics", Syngress, pp. 200, 2014.
[12] T. Shimeall, J. Spring, "Books on Google Play Introduction to Information Security: A Strategic-Based Approach", Newnes, pp. 382, 2013.
[13] B. Shavers, E. Zimmerman, "X-Ways Forensics Practitioner's Guide", Newnes, pp. 264, 2013.
[14] A.T.S. Ho, S. Li, "Handbook of Digital Forensics of Multimedia Data and Devices, Enhanced E-Book", John Wiley & Sons, pp. 704, 2016.
[15] Management Association, Information Resources, "Biometrics: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications", pp. 1852, 2016.
[16] J-S. Pan, P-W. Tsai, H-C. Huang, "Advances in Intelligent Information Hiding and Multimedia Signal Processing: Proceeding of the Twelfth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Nov., 21-23, 2016, Kaohsiung, Taiwan, Volume 2", Springer, pp. 371, 2017.
[17] H.T. Sencar, N. Memon, "Digital Image Forensics: There is More to a Picture than Meets the Eye", Springer Science & Business Media,pp. 372, 2012.
[18] K-Pour, Mehdi, "Encyclopedia of Information Science and Technology, Third Edition", IGI Global, pp. 10384, 2014.
[19] A.T. S. Ho, S.Li, "Handbook of Digital Forensics of Multimedia Data and Devices, Enhanced E-Book", John Wiley & Sons, pp. 704, 2016.
[20] Affinity Photo vs. Photoshop, "https://www.lynda.com/Affinity-Photo-tutorials/Affinity-Photo-vs-Photoshop/453344/473804-4.html", Retrived 08th March, 2017.

[21] "Pixlr Express vs. PicsArt: What's the Best Photography App?" http://heavy.com/tech/2014/07/pixlr-express-vs-picsart-whats-the-best-photography-app/, Retrieved, 08 March, 2017.
[22] "Image Manipulation Dataset", https://www5.cs.fau.de/research/data/image-manipulation/, Retrieved, 08 March, 2017.
[23] J. Engel, V. Koltun, D. Cremers, "Direct Sparse Odometry", Cornell University Library, 2016.
[24] "CASIA v1.0", http://forensics.idealtest.org/, Retrieved, 08 March, 2017.
[25] "Boss Rank", http://agents.fel.cvut.cz/boss/index.php?mode=VIEW&tmpl=materials, Retrieved, 08 March, 2017
[26] "SAO/NASA ADS Physics Abstract Service", http://adsabs.harvard.edu/abs/2003SPIE.5307..472S, Retrieved, 08 March, 2017.
[27] "Image Communication Laboratory", http://lci.micc.unifi.it/labd/2015/01/copy-move-forgery-detection-and-localization/, Retrieved, 08 March, 2017.
[28] M. Zandi, A. Mahmoudi-Aznaveh and A. Talebpour, "Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2499-2512, Nov. 2016.
[29] T. Carvalho, F. A. Faria, H. Pedrini, R. da S. Torres and A. Rocha, "Illuminant-Based Transformed Spaces for Image Forensics," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 720-733, April 2016.
[30] P. Korus and J. Huang, "Improved Tampering Localization in Digital Image Forensics Based on Maximal Entropy Random Walk," in *IEEE Signal Processing Letters*, vol. 23, no. 1, pp. 169-173, Jan. 2016.
[31] P. Korus and J. Huang, "Multi-Scale Analysis Strategies in PRNU-Based Tampering Localization," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 809-824, April 2017.
[32] C.M. Pun, C. Yan and X.C. Yuan, "Image Alignment-Based Multi-Region Matching for Object-Level Tampering Detection," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 377-391, Feb. 2017.
[33] T.H. Thai, R. Cogranne, F. Retraint and T.N.C. Doan, "JPEG Quantization Step Estimation and Its Applications to Digital Image Forensics," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 123-133, Jan. 2017.
[34] V. Conotter, P. Comesaña and F. Pérez-González, "Forensic Detection of Processing Operator Chains: Recovering the History of Filtered JPEG Images," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2257-2269, Nov. 2015.
[35] B. Peng, W. Wang, J. Dong and T. Tan, "Optimized 3D Lighting Environment Estimation for Image Forgery Detection," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 479-494, Feb. 2017.
[36] D. Cozzolino, G. Poggi and L. Verdoliva, "Efficient Dense-Field Copy–Move Forgery Detection," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2284-2297, Nov. 2015.
[37] Y. Li and J. Zhou, "Anti-Forensics of Lossy Predictive Image Compression," in *IEEE Signal Processing Letters*, vol. 22, no. 12, pp. 2219-2223, Dec. 2015.
[38] A. De Rosa, M. Fontani, M. Massai, A. Piva and M. Barni, "Second-Order Statistics Analysis to Cope With Contrast Enhancement Counter-Forensics," in *IEEE Signal Processing Letters*, vol. 22, no. 8, pp. 1132-1136, Aug. 2015.
[39] C. van Dam, R. Veldhuis and L. Spreeuwers, "Face reconstruction from image sequences for forensic face comparison," in *IET Biometrics*, vol. 5, no. 2, pp. 140-146, 6 2016.
[40] W. Fan, K. Wang, F. Cayre and Z. Xiong, "Median Filtered Image Quality Enhancement and Anti-Forensics via Variational Deconvolution," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 1076-1091, May 2015.
[41] J. Li, X. Li, B. Yang and X. Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 507-518, March 2015.
[42] G. Cao, Y. Zhao, R. Ni and X. Li, "Contrast Enhancement-Based Forensics in Digital Images," in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 515-525, March 2014.
[43] A. Costanzo, I. Amerini, R. Caldelli and M. Barni, "Forensic Analysis of SIFT Keypoint Removal and Injection," in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 9, pp. 1450-1464, Sept. 2014.
[44] 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," in *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 593-607, April 2013.
[45] C.T. Li and Y. Li, "Color-Decoupled Photo Response Non-Uniformity for Digital Image Forensics," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 22, no. 2, pp. 260-271, Feb. 2012.
[46] H.M. Sun, C.Y. Weng, C.F. Lee and C.H. Yang, "Anti-Forensics with Steganographic Data Embedding in Digital Images," in *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 7, pp. 1392-1403, August 2011.
[47] W. Luo, J. Huang and G. Qiu, "JPEG Error Analysis and Its Applications to Digital Image Forensics," in *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 480-491, Sept. 2010.
[48] S. Sharma, S.V. Dhavale, "A Review of Passive Forensic Techniques for Detection of Copy-Move Attacks on Digital Videos", 3rd International Conference on Advanced Computing and Communication Systems (ICACCS), 2016.
[49] W.N.N. Diane, S. Xingming and F.K.Moise, "Review Article A Survey of Partition-Based Techniques for Copy-Move Forgery Detection", Hindawi Publishing Corporation, pp. 13, 2014.
[50] M. Ali Qureshi and M. Deriche, "A review on copy move image forgery detection techniques," IEEE 11th International Multi-Conference on Systems, Signals & Devices (SSD14), pp. 1-5, 2014.

[51] R. Poisel, S. Tjoa, "Forensics Investigations of Multimedia Data: A Review of the State-of-the-Art", Sixth International Conference on IT Security Incident Management and IT Forensics, 2016.
[52] C.W. Wang, S.M. Ka and A. Chen, "Robust image registration of biological microscopic images", Scientific reports, Vol.4, pp.6050, 2014.
[53] A. Piva, "An overview on image forensics", ISRN Signal Processing, 2013.
[54] Z. Ting and W. Rangding, "Doctored JPEG image detection based on double compression features analysis," *2009 ISECS International Colloquium on Computing, Communication, Control, and Management*, Sanya, 2009, pp. 76-80.
[55] R. Sekhar and A.S. Chithra, "Recent block-based methods of copy-move forgery detection in digital images", International Journal of Computer Applications, Vol. 89, No. 8, 2014.
[56] V. Schetinger, M. Iuliani, A. Piva, and M.M. Oliveira, "Digital image forensics vs. image composition: An indirect arms race", arXiv preprint arXiv: 1601.03239, 2016.

BIOGRAPHIES OF AUTHORS

Shashidhar TM., Research Scholar, Visvesvaraya Technological University Belagavi, Karnataka, India. Currently pursuing PhD under RVCE (VTU), Karnataka, India. His teaching experience is around 11 years. His research area is Signal Processing. He has completed his M.Tech (Digital electronics and communication system) from PESIT, Bengaluru, Karnataka, India. Also completed B.E. (Electronics and communication), from SJMIT, Chiradurga, Karnataka, India.

Dr. K.B. Ramesh, Associate Professor and Head, Department of Electronics and Instrumentation Engg. R V college of Engineering, Bengaluru, Karnataka, India. He has completed PhD in Computer Science and Engineering from Kuvempu University. He has around twenty three years (23) of teaching experience in E&I Engg. His major research area is in *Computer Science and Engineering and minor* research area is in *Biomedical Engineering/Bioinformatics*.