International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 4, Issue 3, 2017, PP 23-29
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
DOI: http://dx.doi.org/10.20431/2349-4859.0403004
www.arcjournals.org

Image Forensics Techniques for Robust Image Security: A Brief Survey

Harsh Mathur[1], **Dr. S. Veenadhari**[2]

[1]*PhD Scholar, Aisect University*
[2]*Associate Professor, Aisect University, India*

***Corresponding Author:** **Harsh Mathur,** *PhD Scholar, Aisect University. India*

Abstract: *The rising of Cyber Crime has drawn attention toward Digital Forensics and cyber security. it is a branch of forensic science which deals with cyber crime. It essentially includes the detection, recovery and investigation of material found in digital hardware. Digital images and recordings expect most basic part in digital crime scene investigation. They are the prime affirmations of any cyber-crime scene. So the commitment of the image is basic. Digital Photography is having a fast and constantly developing scattering as of late, since it licenses anyone to take a subjective number of good quality images, rapidly and at no cost, and to store them effortlessly on a significant number of digital support, or share them on the Internet. At the same time, with the wide availability of advanced tools for editing image like (e.g. Adobe Photoshop, Gimp), modifying a digital photo, with little or no obvious signs of tampering have become also very easy and widespread. A digitally modified image can be vague from a bona fide image. The altering, be that as it may, may bother some fundamental factual properties of the image. Under this assumption there are many different techniques are proposed that quantify and detect statistical perturbations found in different forms of tampered images. In these literature a comparative analysis and performance of some of them has evaluated.*

Keywords: *Digital Image Tampering, Digital Image Forensic, Image Forgery, Image Authentication, Multimedia Forensics.*

1. Introduction

Digital Forensics has extended to cover examination of all devices fit for putting away digital information. Digital forensics has several applications which includes forensic investigation of digital media devices, intellectual property theft detection and investigation, fraud detection, e-discovery of potential digital evidences and testifying those in courtroom, confirm alibis or statements, determine intent identify sources (e.g., in copyright cases) and authenticate documents.

Digital images and videos are used as the principle form of digital evidences, in the court of law as well as media and broadcast industries. With the progression in advancements and the accessibility of effective image processing devices, the dependability of computerized image is regularly under question. Hence maintenance of their fidelity becomes crucial. ‘

Many types of Digital forgery are being found now days. Like Image Splicing, Image Retouching and Copy move etc. Image splicing is the way toward making a composite picture by cutting and joining at least two photos. The grafted image may present various sharp moves, for example, lines, edges and corners. Image Retouching refers to control for photograph reclamation or upgrade (balancing colors / contrast / white balance (i.e. gradational retouching), sharpness, noise, removing elements or visible flaws on skin or materials). The most primitive form of cyber-attack on digital images is region Duplication. Aim of the attacker is to deceive the viewer with a manipulated image. This is also known as Copy-Move Forgery. In this, a part of the image is copied and pasted somewhere else in the image with the intent to obscure an important feature.

2. Theory of Digital Forensics

Image content can be transformed easily without leaving any visible traces. This has led to the development of image forensic techniques for finding clues within an image to help determine whether the image is original or tampered. Image forensic tools can be classified into one of two main categories: active and passive. Active techniques require the presence of authentication data, embedded in the image during the acquisition process. Passive techniques, on the other hand, rely only on the image content for tamper detection. Detached forensics is expanding in hugeness because of the accessibility of different programming instruments that can be utilized to adjust unique substance without unmistakable follows, and the expanding open attention to such altering. Various passive picture tamper identification frameworks have been proposed in the keeping in touch with, some of which use incorporate extraction procedures for tamper detection and confinement figure 2.1 portray the request of the advanced picture Forgery approaches.

In these days numerous digital phonies are created like Image grafting, modifying and duplicate move Forgery. Picture grafting makes composite picture by joining at least two images. Picture correcting is a procedure of upgrading picture components, for example, sharpness, shading alteration, white adjust and so forth.

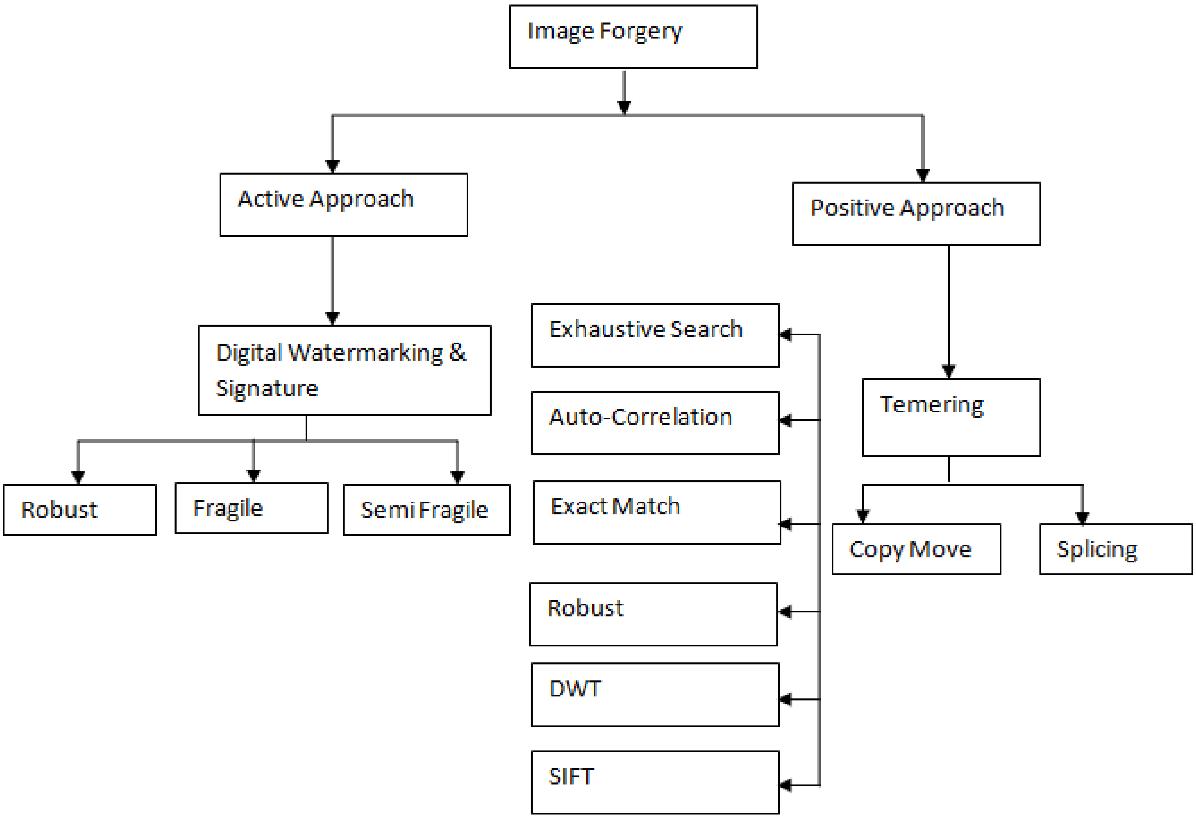

Figure2.1. *Digital Image Forgery Approaches*

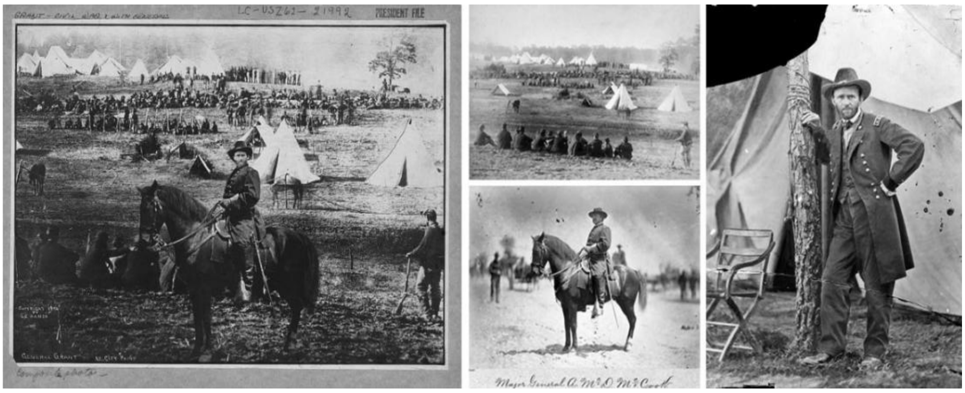

Figure2.2. *One of the earliest examples of photograph manipulation (1864) [10]*

Multimedia content integrity is becoming a major issue of concern nowadays due to the ability to change or modify any type of media such as audio, video or images using any of the abundant multimedia editing software (e.g. Photoshop). Image manipulation goes far back in history. One of the earliest forms of photograph manipulation happened in 1864 when parts from three different images were combined into one composite image. Figure 2.2 shows the composite image on the left (taken during the American civil war) where the face of General Ulysses S. Grant is placed on the body of Major General Alexander M. McCook while riding his horse [1]. The background is of prisoners captured at the battle of Fisher's Hill in Virginia. In the digital age, image manipulation is becoming more common. However, pictures can never again be trusted particularly when utilized as confirmation in an official courtroom since tampering may not be obvious to the bare eye. Along these lines, the field of digital image forensics is engaged towards considering and looking at advanced pictures and asserting authenticity or tampering. In spite of the way that the field of image forensics is a truly new research field, it is broadening rapidly. Many researchers have proposed distinct and effective approaches for image tamper detection.

2.1. Image Tampering

Tampering with images is something neither new, nor later. Probably the most surely understood cases of treating of film photos, for instance, go back to the early years of the previous Soviet Union, where both Lenin and Stalin had "the adversaries of the general population" expelled from notable records, imitations were made utilizing picture controls, for example, enhancing with Photoshop, re-touching, evading and consuming, and complexity and shading modification. During the previous couple of years moderate, high-proficient digital cameras have been rapidly supplanting their film-based, straightforward accomplices. Besides, the presence of simplicity, first class PCs, and modern photograph altering and PC designs programming enable an ordinary customer to do complex picture controls and make dependable computerized fakes without lifting a finger. Despite the fact that there are, possibly, an uncountable number of ways to deal with control and mess with computerized images, we display here probably the most well-known sorts of advanced picture tampering [11].

2.2. Watermarking

The Watermarking has been characterized as "the demonstration of impalpably changing a Work to embed a message about that Work", where Work alludes to a particular picture, sound clasp, video cut, or other advanced media [12]. The essential approach utilizes an implanted that embeds a subtle watermark (e.g., an advanced code, or a checksum) into the media, and a decoder that tries to decide whether a watermark is available, and assuming this is the case, yields its encoded message.

Digital watermarking has various applications, including: impart checking, owner identification evidence, possession confirmation, exchange following, content verification, and duplicate and device control. In spite of the fact that not by any means the only answer for these applications, advanced watermarks are recognized from different systems by three characterizing qualities: (1) they are vague, (2) they are indistinguishable from the computerized media they are implanted in, and (3) they experience an indistinguishable changes from the digital media itself.

3. Related Work

A. Dada Warbhe, R. V. Dharaskar and V. M. Thakare, [1] Introduce a digital image forensic technique which can identify one of such picture tampering. As images can be tampered in different ways, address a commonplace case called as copy stick modifying. Our proposed system is intense to relative change; especially to upset and scaling.

It ended up being easy today to catch and make advanced photographs. It's no more a costlier issue, as a vast segment of the handheld electronic gadgets; for instance, mobile phones are outfitted with digital cameras. Today, there are adequate PC and convenient applications open which are made to control received photographs. One can undoubtedly take a photo, control it with the introduced application and make it viral through the web. Consequently, these computerized photos ought not be deciphered as they talk. Digital images are the great confirmation of occasions and places. Consequently, these digital photos can be displayed as confirmation under the steady gaze of an official courtroom. It ends up being basic in such cases at that point, to exhibit the digital photographs being referred to be one of a kind. Digital picture crime scene investigation expect an essential part in such conditions. Digital picture crime scene investigation is a branch of digital legal sciences which oversees assessing the digital photographs for their credibility and trustworthiness.

A Coherence Based Forgery Detection (CBFD) technique has been proposed by Meenakshi Sundaram A and C. Nandini, [2] in the current circumstances different malicious assaults can be performed over images for copying the images which presents huge measure of difficulties in the area of forgery detection and highlight based image confirmation. Scientists have concentrated on the improvement of effective image falsification discovery systems which can be relevant to streamline image modifying assaults. The current research trends also focus on the authenticity of an image. The proposed technique isolates the info image into fragmented squares and concentrates include vectors from the measurably sorted framework. The proposed strategies additionally utilizes include vectors and the separation between highlight vectors for guaranteeing the suspicious squares introduce in the image. The test investigation demonstrates that the proposed framework achieves better accuracy in detection of forged regions even if it is blurred with the use of Gaussian blurring which hides the forged and suspicious blocks of an image [2].

Digital images are anything but difficult to control and alter because of advances in PCs and picture altering programming. Duplicate move imitation is a champion among the most surely understood tampering ancient pieces in digital images that used by picture falsifiers. E. Mohebbian and M. Hariri, [3], developed a DCT-based method to recognize picture imitation considering the multifaceted nature of data picture. To perceive copy, images are isolated into two classes: smooth and complex. To concentrate highlights discrete cosine change (DCT) is connected to each square. Demonstrated Experimental outcomes that proposed technique can correctly distinguish copied areas notwithstanding when the image was experienced a few image controls like lossy JPEG pressure, Gaussian obscure sifting and Gaussian background noise [3].

When creating a digital forgery, it is often necessary to combine several images. Image splicing is one such type of tampering. As of late, specialists have proposed different strategies for distinguishing such splicing. F. Zeng, W. Wang, M. Tang and Z. Cao,[4], propose a novel method for blurred image splicing localization based on blind image restoration. Utilize blur parameters estimation through the spectrum attributes of blur images with a particular true objective to restore the joined area and whatever is left of the image. Likewise build up another measure to aid conflicting locale division in reestablished images that contain a lot of ringing impact [4]. Exploratory outcomes demonstrate adequacy of the strategy regardless of the possibility that the images to be tried have been noised or compacted with a low quality element block chart of the stream of technique has outlined in figure 3.1.

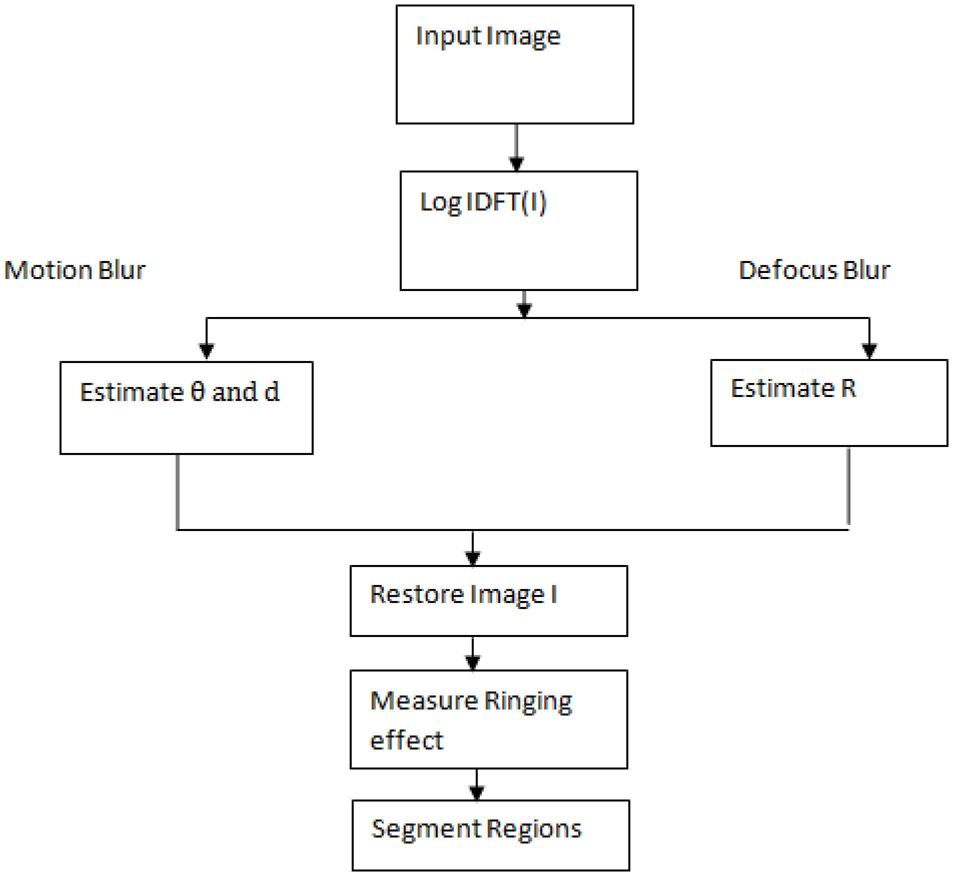

Figure3.1. *Flow chart of splicing detection method. [4]*

Region duplication has turned out to be normal in image forgery attributable to the accessibility of cutting edge altering programming and completely prepared digital cameras. Most existing square based duplicate move detection procedures battle to identify such alters under post processing operations, such as scaling and JPEG compression. This study D. M. Uliyan, H. A. Jalab and A. W. A. Wahab, [5] proposes a copy-move image forgery detection algorithm using Hessian features and a center-symmetric local binary pattern (CSLBP). The proposed technique comprises of four stages: (1) identifying the object based on normalized cut segmentation, (2) localizing the local interest points of each object based on the Hessian strategy, (3) extracting CSLBP elements, and (4) recognizing duplicated areas in image falsifications. Experiment results show that the method is robust to post processed copy-move forgery under scaling, and JPEG compression figure 3.2.

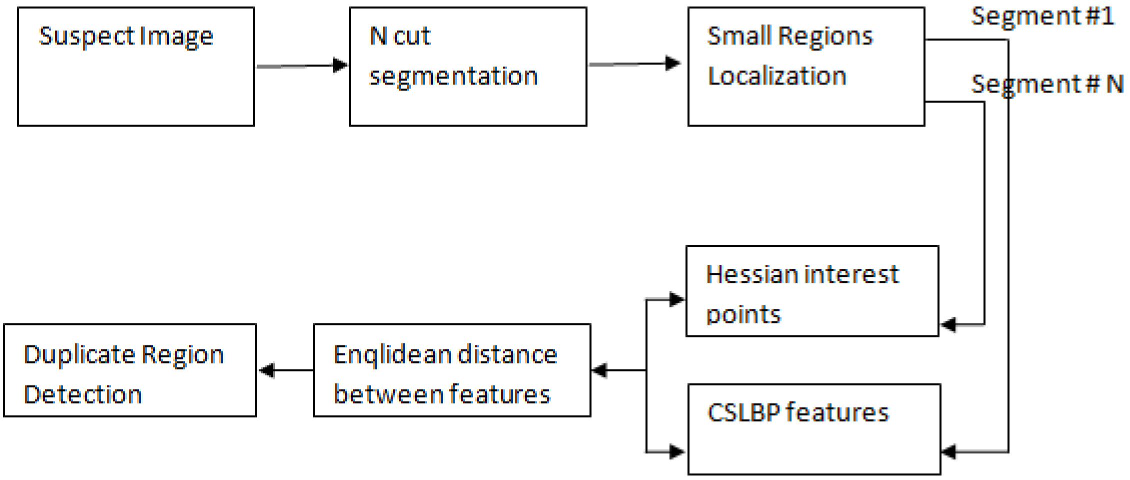

Figure3.2. *Hessian method of CSLBP features detection Region duplication model [5]*

These days a few changes on the digital images are made with the quick advancement of image altering apparatuses as of late. The most well-known technique in the adjustments made is copy-move forgery. Greater part of the proposed strategies to distinguish copy-move forgery in the writing depend on square and not impervious to different geometric changes before moving adapted image . For the objective regarding to this , key points of each channel of forged color image are extracted by using Colour SIFT that is the key point -based method . B. Üstübioğlu, S. Ayas, H. Doğan and G. Ulutaş, [6] study the comparison between SIFT and Colour SIFT is made. More successful forgery detection is made by getting more coordinating focuses utilizing Color SIFT than SIFT is found in the correlation comes about. Besides, proposed technique identifies fashioned image amid turn, scaling, JPEG pressure is appeared in the outcomes [6].

D. Cozzolino, G. Poggi and L. Verdoliva,[7] propose another algorithm for copy-move forgery detection and confinement, in view of the quick calculation of a thick closest neighbor field. To this end, utilize PatchMatch, an iterative randomized algorithm for closest neighbor search, which abuses the normality of characteristic images to unite quickly to a close ideal and smooth field. Adjust the essential algorithm to pick up power against turns, while keeping the first computational effectiveness. Experimental results demonstrate the proposed method to beat almost uniformly all tested reference techniques as far as both accuracy and speed.

The goal of copy-move forgery detection strategies is to discover copied regions inside a similar image. There are two fundamental ways to deal with distinguish copy-move forgery: key point-based and block based techniques. In spite of the fact that the previous is predominant as far as computational multifaceted nature, these techniques disregard the smooth districts since they limit their pursuit to notable focuses. Then again, while square based strategies consider smooth zones, they present a colossal number of false matches. M. Zandi, A. Mahmoudi-Aznaveh and A. Mansouri,[8], is proposed to utilize a adaptive threshold in matching phase with a specific end goal to conquer this issue. The test comes about show that the proposed technique can extraordinarily decrease the quantity of false matches which brings about enhancing both execution and computational cost Figure 3.3 demonstrate Common copy-move forgery detection system architecture.

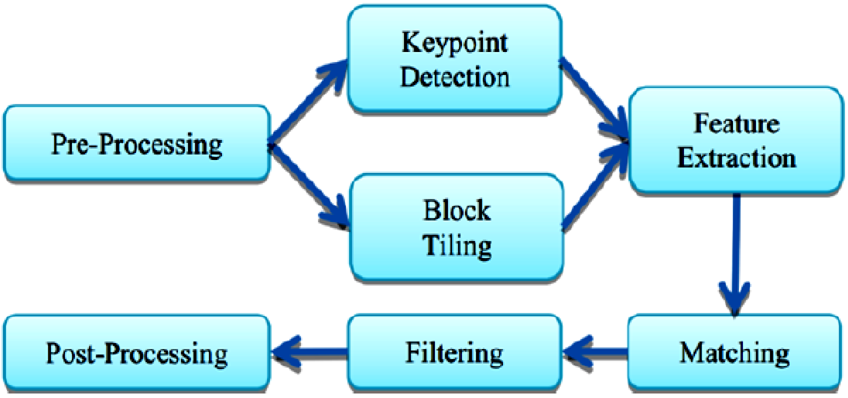

Figure3.3. *Common copy-move forgery detection system architecture [8]*

4. Problem Statement

Customarily, it is considered that images are trustworthy as it captured through traditional analog camera devices to depict the real-world happenings. This traditional trustworthiness is built on remarkable difficulties of image content modification. Indeed, modifying the content of a film-based photo requires special skills, yet time-consuming and costly, through dark room tricks. Therefore, this modification is of limited extent.

The past decade have witness of the evolution of digital imaging technology with a dramatic improvement of digital images' quality. This improvement is not only due to advances in semiconductor fabrication technology that makes it possible to reduce the pixel size in an image sensor and thus raises the total number of pixels, but also advances in image processing technology that allows reducing noise introduced in a camera and enhancing details of the physical scene. The digital revolution largely replaces their analog counterparts to enable ease of digital content creation and processing at affordable cost and in mass scale. Unfortunately, this path of technological evolution may provide means for malicious purposes. Digital images can be effectively altered, changed or distorted in view of a vast accessibility of minimal effort image altering apparatuses. Thusly, misrepresented photos are showing up with a developing recurrence and modernity.

5. Conclusion

In our work we have considered several techniques – like Exhaustive Search, Autocorrelation, Exact Block Matching and Detection Duplication Algorithm using Principal component analysis. Copy-Move forgery is a dynamic field in which a lot of researchers are working on and have successfully implemented different techniques. All these techniques are block based techniques and have various positives and negatives like Exhaustive Search suffers from high time complexity and fundamental component analysis approach has very good accuracy results but it suffers from False Positives. So, when it comes to - which technique to choose for a particular type of forged image - then this parameterization will help the user. On the basis of requirement, one can use a particular unit block size and a particular technique. From our simulation results, it is clear that Detection Accuracy is inversely proportional to unit block size and for larger forgery the detection accuracy will be high. For False negative it is just opposite to that of detection accuracy i.e. directly proportional to block size. For the first three techniques that we discussed False Positive for them was zero but in the fundamental component analysis approach have high accuracy but face a small False Positive rate so there is a tradeoff between Detection Accuracy and False positive.

References

[1] A. Dada Warbhe, R. V. Dharaskar and V. M. Thakare, "Digital image forensics: An affine transform robust copy-paste tampering detection," 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, 2016, pp. 1-5.

[2] Meenakshi Sundaram A and C. Nandini, "CBFD: Coherence Based Forgery Detection technique in image forensics analysis," 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), Mandya, 2015, pp. 192-197.

[3] E. Mohebbian and M. Hariri, "Increase the efficiency of DCT method for detection of copy-move forgery in complex and smooth images," 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, 2015, pp. 436-440.

[4] F. Zeng, W. Wang, M. Tang and Z. Cao, "Exposing Blurred Image Forgeries through Blind Image Restoration," 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Krakow, 2015, pp. 466-469.

[5] D. M. Uliyan, H. A. Jalab and A. W. A. Wahab, "Copy move image forgery detection using Hessian and center symmetric local binary pattern," 2015 IEEE Conference on Open Systems (ICOS), Melaka, 2015, pp. 7-11.

[6] [6] B. Üstübioğlu, S. Ayas, H. Doğan and G. Ulutaş, "Image forgery detection based on Colour SIFT," 2015 23nd Signal Processing and Communications Applications Conference (SIU), Malatya, 2015, pp. 1741-1744.

[7] D. Cozzolino, G. Poggi and L. Verdoliva, "Copy-move forgery detection based on PatchMatch," 2014 IEEE International Conference on Image Processing (ICIP), Paris, 2014, pp. 5312-5316.

[8] M. Zandi, A. Mahmoudi-Aznaveh and A. Mansouri, "Adaptive matching for copy-move Forgery detection," 2014 IEEE International Workshop on Information Forensics and Security (WIFS), Atlanta, GA, 2014, pp. 119-124.

[9] Fridrich, A. Jessica, B. David Soukal, and A. Jan Lukas. "Detection of copy-move forgery in digital images." in Proceedings of Digital Forensic Research Workshop. 2003.

[10] Prints & Photographs Division Library of Congress. Photo tampering throughout history. URL http://www.fourandsix.com/photo-tampering-history/.

[11] H. Farid. Creating and detecting doctored and virtual images: Implications to the child pornography prevention act. Technical Report TR2004-518, Dartmouth College, September 2004.

[12] I.J. Cox, M. L. Miller, and J. A. Bloom. Digital Watermarking. Morgan Kaufmann Publishers, 2002.

Citation: *Harsh Mathur & Dr. S. Veenadhari (2017). Image Forensics Techniques for Robust Image Security: A Brief Survey, International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), 4(3), pp.23-29, DOI: http://dx.doi.org/10.20431/2349-4859.0403004*