Survey on Recent Image Forgeries and their Detection Methods

[*]Vinay D Mohite, [#]Uttara Athawale, [$]Sonali Athawale

[*]Student, [#]Professor, [$]Assistant Professor, Bharati Vidyapeeth, Navi Mumbai, India,

[*]mohitevinay910@gmail.com, [#]uttara.athawale @gmail.com, [$]sonali.athawale @gmail.com

ABSTRACT-In recent years, with the improvement of digital manipulation tools, image forgeries have become a social issue. Copy-move forgery is an important type of digital manipulation which is done by duplicating some parts of the image with the purpose of hiding specific information. Research in the area of image forensics is driven by the enormous image forgery done these days. Numerous algorithms are used for image forgery detection. This paper is an attempt to review the types of the image forgeries, and the recent methods adopted to identify them, real world popular examples of image forgery, special focus is given on copy move forgery and digital cheque image forgery.

Keywords — Copy-Move, CTS, DCT, Image Forgery, Image Retouching, photomontage, RANSAC, SVM, SIFT.

I. INTRODUCTION

In today's world Digital images play a significant role in our everyday life. Digital Image forgery is the process of making illegal changes in images, image information. The applications that use digital images are more prone to forgery because it is easy for the user to edit the image by the image editing tools that are widely available in market [7]. Image manipulation has become quite simple by the advent of powerful digital image processing programs and applications such as Photoshop have made the tampering of digital images even more easier and a common practice[37] Thus making digital forgeries from one or multiple images has become easy. In today's era fake images are often created to for political motives. We come across thousand of images that are digitally manipulated. There are certain images that throughout our history have been considered to be trustworthy. These images may have been presented as supporting evidence and may have been used in various fields, such as in digital forensic investigation, journalistic photography[3]. Today, the authenticity of mage is questionable particularly if the images are used in a court of law, news reports, and insurance claims. [93]

Different types of research is done in digital image forensics with the concern of digital image authentication. Also, various methods have been proposed over years to detect image forgery [5],[45]

In Digital world, Image Forgery is a real time issue in this present era, which causes a lot of tribulations to the society. The forgery in an image includes object addition, object removal and changing color etc. Image Forgery detection is a new area of research in digital image forgery detection technique [4]. Figure1 shows the original and forged image which is easily done with the available tools in the market

Today, image authenticity is a matter of tremendous concern. Several image forensics techniques are used for the same. They can be broadly classified as active forensic technique and passive forensic technique.[53],[97],[100]

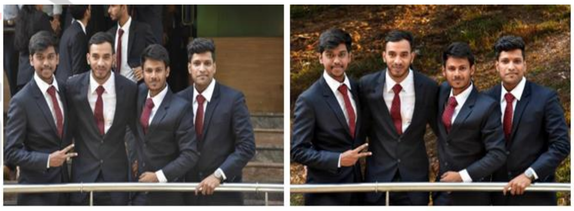

Figure 1: a) Original b)Forged

In Active forensic technique, watermarking and steganography are two techniques which are used to insert authentic information into the image. When question arises about the authenticity of an image, then prior embedded authentication information is recalled to prove the authenticity of that image. However, embedding authentication information to an image is very confidential. One of the limitations of Active forensic technique is applying multiple steps of processing of digital image. In passive forensic techniques, the most popular method to construct forged image is copy-move forgery. It refers to copy one part from image and paste it inside the same image [1]

Digital image copy-move forgery is the most frequently used type of image manipulation.[62] Copy-move manipulation is forging an image by duplicating a particular portion of the digital image with the purpose of hiding some information of the same digital image.[35]

The capability to locate the manipulated parts of the image can be handy in different forensic situations such as crime scene investigations. One of the standard methods for detecting the forged regions is to calculate the arithmetical characteristics of various sections of the image and compare

DOI : 10.35291/2454-9150.2019.0148

the results with each other. Some of the limitations faced by the current copy-move detection algorithms struggle are lack of robustness to post-processing operations; detection algorithms need to be robust to all pre-processing operations such as rotation, scaling, noise and JPEG compression. Secondly, the algorithms are unable to detect multiple forgeries; it is essential for a detection method to be able to detect forgery in cases of multiple cloning. Also, forgery detection rate to precisely locate the forged regions is low the detection scheme needs to have the higher true positive rate in locating procedure [8],[5], [9], [10].

Image forgery techniques are applied in various areas for authentication of images captured from various sources like CCD (Charge Couple Device) cameras, authentication of vital information in an image, authenticity of evidences, Fingerprint Recognition, Document Authentication.[7] Rapid advances in modern scanning technology have greatly simplified the task of converting documents to a digital format. Some digitized documents are very important and their unauthorized use could result in monetary, organizational, social or individual losses.

Among the various areas, the most dangerous image forgery is done on the bank cheques that can result in large monetary loss. One of the areas of concern in online banking system is a digital cheque forgery attack on cheque processing systems that results in cheque fraud. The multiple factors that facilitate the cheque fraud are the use of digital images to perform cheque transactions, advances in image processing technologies, the use of untrusted client-side devices and software, and the modalities of deposit. The digital cheque forgery attacks offer better chances of success in committing fraud as compared to the conventional cheque forgery attacks. Image processing provides an attacker with the opportunity to manipulate an image at the pixel level with a level of precision unrivaled by physical forgery. [46],[64]

There are numerous historical evidences of physical cheque forgery and the losses are increasing day by day. According to the Australian Payment Clearance Association losses due to fraudulently-altered cheques in 2015 were 80% more than the losses in 2013. Moreover, losses due to non-originated counterfeit cheques in 2015 registered a three-fold increase over 2013. In India, the Reserve Bank of India reported that 1,197.2 million bank cheques were cleared during the 2015-2016 fiscal year. In another report, the Reserve Bank of India estimates that losses due to bank fraud nearly doubled from INR 10.071 billion during the 2013-14 fiscal year to INR 19.361 billion during the 2014-15 fiscal year [49]

Prior to use of digital cheque, the physical cheque transactions included the flow of movement of cheque physically from one bank to another for cheque clearing process. This required more time and could be tampered while going through the entire process and was in secure. In India, RBI uses cheque truncation system (CTS) or Image based Clearing System ICS is used to speed the process for fast clearing of cheques. [47],[63], CTS transforms this physical transmission to digital. An electronic image of the cheque is sent to the paying bank through the clearing house including some relevant information needed[83],[102]. It enables the customer and banks with many benefits like shorter clearing cycle, security, verification process and many more [63]

It is more secure and the information is been encrypted while passing it through the digital format. The scanned copy of the cheque is also been stored in database for future references. This is been done for storing the information so that it can be reverted if needed. Despite of the security, attempts have been made to forge the digital cheques also. Recently a image forgery attack was detected in Kolkata. a gang of bank fraudsters forged cheques so neatly that they faked even the magnetic ink character recognition data.[42] The point of concern is that the gang was able to dodge the image based clearing system that is used by banks as per the Reserve Bank of India mandates. [42]

II. MAJOR TYPES OF IMAGE FORGERIES

1. **Image Retouching:** Image Retouching is a less harmful kind of digital image forgery. Image is not changed significantly, but it employs image enhancement. The original image is modified and certain features are changed. This technique is popular among magazine photo editors and is present in almost all magazines. [64] Even though it is used only for making pretty photographs and it is not harmful type of image forgery, the fact remains that such enhancement is ethically wrong.[7],[64], [45]

2. **Image Splicing Or Photomontage:** It involves merging of two or more different images to form a combined image that is significantly different from the original image. It is more harmful than Image retouching. Image splicing can be done by pasting part of the image regions from the same or separate sources images. [45]A fake image is produced by sticking, together two or more images using digital tools available such as Photoshop. Several infamous news reporting cases that involve the use of faked images is a common example of image splicing. The below figure shows a forged image created by copying a spliced portion from the source image into a target image. [44], [7],[64]

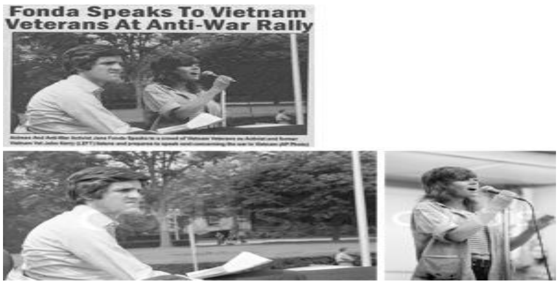

Figure 2: John Kerry and Jane Fonda (**Image Splicing) Image downloaded from [68]**

COPY-MOVE FORGERY: The copy move forgery also known as cloning is one of the difficult but most commonly used image tampering technique [35], a part of the image is covered by another part of the image itself. [92] In a copy-move attack, the main purpose is hiding the information in the original image with some other part of the same image. [64] Thus the desired information can be added or hidden by covering it by a part of the image. The example of Copy-Move type is as shown in below figure. The original image contains only three missiles and its fake image is created using Copy-Move technique on the right has four missiles. [7], [64]

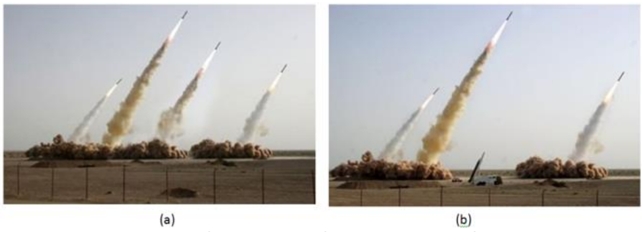

Figure 3: An example of copy-move forgery: (a) the forged image with four missiles & (b) the original image with three missiles. Image downloaded from [48]

III. COPY –MOVE FORGERY DETECTION METHODS

In copy Move forgery a block of the picture is replicated and stuck to another block of a similar picture Thus, it is it extremely difficult to recognize this type of fabrication as the replicated image is taken from a similar image. [6], [59],[65], [66], [76] In this section we survey different methods used in detecting copy move forgery

a) **SVM Classifier:** SVM classifier is one of the most effective data mining algorithms. It is similar to the functional form of neural networks and radial basis functions. SVM uses a training dataset to train the algorithm which is used to determine if the class for a tested image is a forged or an original image. The algorithm use some features to be extracted and then exploited in the classification process [2].

b) **Discrete Cosine Transform (DCT):** Discrete Cosine Transform (DCT) is a block based method is used to detect the forged images. It is used to locate the doctored parts in the image. DCT algorithm uses the divide and conquers technique by dividing the image into overlapping blocks. Using DCT, duplicated regions can be easily identified in the image.[6] DCT is simple and fast and widely used for matching duplicated, overlapped regions[6],[59],[62]

c) **Block-Based Methods :** This Block-based algorithm divides the digital image into overlapped blocks of a specific size and feature vector that will be computed as a hash value for each and every block to match the differences to detect if the digital images have a duplicated region or not [11]. Block-based approach makes use of algorithms such as DCT, DWT, KPCA, PCA and ZERNIKE [67],[95],[96]

d) **Genetic Algorithm (GA):**Genetic algorithm (GA) is used to generate the high quality solutions for optimization by selecting the most suitable and the minimum number of features in the image to localize the tampered regions by using the Euclidean distance between them. This algorithm has a high performance in detecting a copy-paste image forgery [12]. GA is proven as more accurate and effective algorithm for detecting the image forgery, [59][6]

e) **Brute Force:** Brute force method uses searching the matching segment with its circularly shifted versions; As the search is exhaustive, the number of comparisons is very high, its computational cost can be very high. [76] Further, auto correlation is used to determine the location change of the image segment. [76]

f) **Key point Based Method:** Key point Based Method: unlike block based methods that operate on blocks of a image, Key point based technique operates on the whole image. Key point based methods compute their attributes only on picture areas with excessive disorder. [80]

Key point based method are be further classified into two techniques:

i. **SIFT** (scale invariant feature transform): The Scale-Invariant Feature Transform (SIFT) is used to detect & describe local features in an image. The keypoints of the suspected forged image are extracted and analysed with keypoints generated from all over the image for similarity matching.[82]

ii. **SURF** (Speeded Up Robust Features) The Speed Up Robust Feature detector (SURF) ensures the high speed in three of the feature detection steps: detection, description, and matching. Due to the use of the Hessian matrix's trace, the matching speed has been significantly improved over the SIFT. The SURF algorithm speeds up the SIFT's detection process without scarifying the quality of the detected points.[61]

g) **False Positive Removal(RANSAC) :**Random Sample Consensus algorithm (RANSAC) removes false positive matches. In RANSAC algorithm, a set of matched points are randomly selected and then the homography is estimated. After that other remaining matched points are transformed and then compared in terms of distance with respect to their respective matches. A threshold value is set. If this distance is under the threshold value it is marked as inliers and if it is above the threshold is catalogued as outliers. After a predefined number of iterations, the estimated transformation which is associated with the higher number of inliers is chosen [13]

DOI : 10.35291/2454-9150.2019.0148

IV. Examples of Digital Image Forgery in Real World

Image Forgery is used in real world dates back to the time when physical photographic images were first created. But before the digital age, such tampering required a very high level technical expertise, specialized equipment and was a time-consuming Examples of physical photo tampering throughout history, starting in the mid1800s. But since the advent of digital imaging, today's technology allows digital media to be altered and manipulated in ways that were simply impossible 20 years ago. [74] Table No. 1 lists some of the real world popular examples of image forgery, its type and the method used for forgery detection. [73]

Table No. 1 Some of the real world popular examples of image forgery, its type and the method used for forgery detection.[48]

Sr.No.	Year	Broad type of forgery detection method Used	Forgery Attacks	Examples
1	2003	DCT, Pixel-based techniques	Copy Move Forgery, Image retouching	The composite image used three different images: The White House, Bill Clinton, and Saddam Hussein. The White House was rescaled and blurred for background illusion creation. Then, images cuts of Bill Clinton and Saddam were pasted on it.[70], [71]
2	2003	DCT, Pixel-based techniques	Image Splicing	A British soldier is pictured in Basra urging Iraqi civilians to stay down and take cover. The staff photographer, Brian Walski combined two of his photographs to "improve" the composition. [72],[101]
3	2004	DCT ,Pixel-based techniques	Image Splicing	John Kerry and Jane Fonda sharing a stage is a digital composite of Kerry taken in Mineola, N.Y., in June 1971. and Jane Fonda in Miami Beach, Fla., in August 1972., [48], [69] ,[75] (image in Figure 2.)
4	2008	DCT	Copy Move Forgery (cloning)	Iranian missile test, the second missile from the right was digitally added to the image to conceal a missile on the ground that did not fire. [73], [101] (image in Figure 3.)
5	2010	Object Removal methods	Image Hidding	Photo of injured Israeli commando lying on the deck , one of the men surrounding the commando was holding a knife, after omission of the knife, the photo that was released[73]
6	2010	Object Removal methods	Image Hidding	Winston Churchill trademark cigarette has been removed when it was featured at The Britain At War Experience museum in London [48] ,[69], [73], [101]
7	2011	Object Removal methods	Image Hidding	Spanish sports newspaper photograph of a match between spanish teams Athletic Bilbao and Barcelona displayed a forged photo in which the defender had been removed[73]
8	2012	Different image enhancement techniques	Image Retouching	The L'Oreal advertisment of anti-wrinkle cream was substantially retouched to make the featuring actress Rachel weisz complexion smoother. it was banned by the British Advertising Standatds Autority (ASA) [73]
9	2013	SIFT Affine Transformation	Cloning an area of image into another zone	Syrian Opposition fighter attacks during an exchange of fire with government forces in Telata Village A video camera that was visibe in the frame was removed [13], [48] [73], [101]
10	2013	Object Removal methods	Image Hidding	Local newspaper in Sichuan region published a manipulated photo which depicted that the communist party secretary was standing in the middle of his own shadow. They had deleted the photo of a photographer who was standing behind the secretary. [73]
11	2015	DCT, Pixel based techniques	Copy Move Forgery, Image Splicing	California lawyer had posted forged pictures of her with a variety of celebrities that were composites of different images in which she had inserted herself. [73]
12	2015	DCT, Pixel based techniques	Copy Move Forgery	British Prime Minister David Cameron wearing a remembrance day poppy. The poppy was crudely pasted over an existing photo. [48],[73], [101]
13	2015	Object Removal methods	Image Hidding	The baby gorilla image had been modified to remove a stary piece of straw.The News Corp photgrapher David Caird withdrew this entry for the photographer award after the judges discoverd it. [73]
14	2016	Pixel-based techniques	Copy Move Forgery	The photographer Yu Wei added the image of a plane perfectly framed within the scaffolding of a fire escape in the competition for the facebook page held by Nikon in Singapore [73]
15	2017	DCT ,Pixel-based techniques	Image Splicing	A photograph showing Marilyn Monroe and Elizabeth Taylor posing together while leaning against a tree was posted to Twitter by @HistoryInMoment on 16 April 2017, This image is a composite of two long-buried photographs that were doctored to show the two icons leaning against a tree together. [78] , [79]
16	2018	DCT, Pixel based techniques	Copy Move Forgery	Fight Fake News [77]

DOI : 10.35291/2454-9150.2019.0148

V. SURVEY OF IMAGE FORGERY DETECTION TECHNIQUES FROM RESEARCH PAPERS AND ARTICLES

The research is done on image forgery detection in image is massive, many algorithms can be used to detect forged images[50]. Below Table No.2 classifies the type of copy move forgery and the techniques used to detect in some recent research papers.[74]

Table No. 2: Classification of type of Image forgery detection techniques

Sr. No	Year	Title of the research paper	Forgery detection technique(s)
1	2012	Blind copy move image forgery detection Using dyadic undecimated wavelet transform [14]	Dyadic undecimated wavelet transform
2	2012	A fast image copy-move forgery detection method using phase correlation [15]	Phase correlation
3	2012	An evaluation of popular copy-move Forgery detection approaches [16]	DCT, DWT, KPCA, PCA, and Zernike
4	2012	Detection of copy-move forgery in digital images Using radon transformation and phase correlation [17]	Radon transformation and phase correlation
5	2012	Detecting image splicing using merged features in chroma space [34]	DCT, Markov
6	2012	Pixel Based Digital Image Forgery Detection Techniques[88]	DWT, feature vector Pixel Based techniques
7	2012	Efficient Copy-Move Forgery Detection for Digital Images [33]	Fourier Transform
8	2012	Exposing Post processed Copy–Paste Forgeries Through Transform-Invariant Features [36]	Transform invariant features, MPEG-7 image signature tools
9	2013	A robust image copy-move forgery detection Based on mixed moments [18]	Mixed moment, Gaussian pyramid transform
10	2013	A fast DCT based method for copy move forgery Detection [19]	DCT
11	2013	Copy move forgery detection using DWT and SIFT features [20]	DWT and SIFT
12	2013	Copy move image forgery detection method using Steerable pyramid transform and texture descriptor [21]	Steerable pyramid transform local binary pattern (LBP)., and texture descriptor [74]
13	2013	Copy move image forgery detection using mutual Information [22]	Mutual Information of different regions of an image
14	2013	Copy-move forgery detection in images via 2D-fourier transform [23]	2D- fourier transform
15	2013	Copy-move image forgery detection using local binary pattern and Neighborhood clustering [24]	Local binary pattern and Neighbourhood clustering
16	2014	Image Forgery Detection Based on Semantics [41]	Framework semantic ontology commonsense knowledgebase
17	2014	Tampering and Copy move forgery detection using shift Feature" [40]	SIFT Duplicated and localization.
18	2014	A copy-move image forgery detection based on speeded up robust feature transform and wavelet Transforms [25]	Speeded up robust feature transform and wavelet Transforms
19	2014	A scheme for copy-move forgery detection in Digital images based in 2D-DWT [26]	2D-DWT
20	2014	Copy-rotate-move forgery detection based on Spatial domain [27]	Spatial domain
21	2014	Copy-rotation-move forgery detection using the Mrogh descriptor [28]	Mrogh descriptor
22	2014	JPEG copy paste forgery detection using BAG optimized for complex images. [29]	Bag Optimized for complex images
23	2014	Shape based copy move forgery detection using level set approach [30]	Level set approach
24	2014	Copy-move forgery detection based on PatchMatch [43]	Localization, nearest neighbour
25	2015	Detection of splicing forgery using wavelet decomposition [31]	wavelet decomposition
26	2016	Forensic Analysis of Copy-Move Forgery in Digital Images Using the Stationary Wavelets [56]	PCA,DCT,DWT,SWT
27	2016	Detection of Digital Image Forgery using Wavelet Decomposition and Outline Analysis [51]	Wavelet Decomposition
28	2016	Novel approach for Image Forgery Detection Technique based on colour illumination using machine learning approach[32]	Machine learning
29	2016	Detection of copy move forgery using Legendre Moments [94]	Legendre Moments and feature vectors
30	2017	Development of Photo Forensics Algorithm by Detecting photoshop Manipulation Using Error Level Analysis [54]	Pixel Based Technique, error level analysis vertical and horizontal histograms
31	2017	A Hybrid Technique For Copy-Move Forgery Detection In Digital Images[95]	Hybrid (DCT, SURF)
32	2017	An efficient ward-based copy-move forgery detection method for digital image forensic [5]	SIFT, ward-based clustering
33	2018	Detecting Splicing and Copy-Move Attacks in Color Images [52]	DCT, LBP(local binary pattern)
34	2018	Copy-move Image Forgery Detection Based on Gabor Descriptors and K-Means Clustering [1]	N-Cut Segmentation
35	2018	Image Forensic for Digital Image Copy Move Forgery Detection [3]	SIFT and SURF

DOI : 10.35291/2454-9150.2019.0148

36	2018	Framework For Image Forgery Detection And Classification Using Machine Learning [60]	GLCM, Machine Learning methods
37	2018	A Tale of a Deep Learning Approach to Image Forgery Detection[39]	Binary classification, Deep learning
38	2018	Digital Image Forensics Technique for Copy-Move Forgery Detection Using DoG and ORB [98]	Difference of Gaussian, Oriented Fast and Rotated Brief
39	2019	A Modern Approach for Image Forgery Detection using BRICH Clustering based on Normalised Mean and Standard Deviation [57]	Cluster based BRICH algorithm
40	2019	Hybrid LSTM and Encoder-Decoder Architecture for Detection of Image Forgeries [99]	Hybrid LSTM, Deep Learning

Besides this, numerous Research articles have been published on image forgery and many effective methods have been proposed to detect such forgeries. To name a few, image algorithms that use radix sorting, Fuzzy Transform, Ring Projection Transform , Discrete Wavelet Transform, Singular Value Decomposition are some of the novel methods [60]

VI. Conclusion

The capabilities and the availability of image editing tools help to make the forged images to be widespread.

People have also used such tools to doctor images for deceptive purposes such as manipulating important official documents and even digital cheques. Some real world examples of image forgery are quoted in this paper and many more such forged images are floating on social media. The survey of research papers of image forgery detection shows that numerous methods are developed for detecting image forgery, but with the advancement of image editing software, dealing with tampered images has become one of the most serious needs of the digital age. Thus, there is an increasingly urgent need for developing more effective and robust image forgery detections methods. Today, abundant research is being done in the area of artificial intelligence, image mining, machine learning and deep learning. The research in these areas should be used for devising new efficient image forgery detection methods to combat the growing number of tampered of images on social media.

References

[1] H. M. S. Parvez, S. Sadeghi, H. A. Jalab, A. R. Al-Shamasneh and D. M. Uliyan, “Copy-move Image Forgery Detection Based on Gabor Descriptors and K-Means Clustering,” 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Shah Alam, 2018, pp. 1-6.

[2] Anita Sahani and K.Srilatha, "Image Forgery Detection Using Svm Classifier", Vol. 3, Issue 3, March 2014 .

[3] Y. Y. Yeap, U. U. Sheikh and A. A. A. Rahman, "Image forensic for digital image copy move forgery detection," 2018 IEEE 14th International Colloquium on Signal Processing & Its Applications (CSPA), Batu Feringghi, 2018, pp. 239-244.

[4] Shikha Dubey , Anshul Sarawagi , Manish Shrivastava ,“Image Forgery Detection based on Local Descriptors and Block-Matching using Clustering Technique,” 2016 International Journal of Computer Applications, vol. 141, no. 10,pp. 11-14

[5] S. Dadkhah, M. Koppen, S. Sadeghi, K. Yoshida, H. A. Jalab and A. A. Manaf, “An efficient ward-based copy-move forgery detection method for digital image forensic,”2017 International Conference on Image and Vision Computing New Zealand (IVCNZ), Christchurch, 2017, pp. 1-6.

[6] Ashima Gupta, Nisheeth Saxena and S.K Vasistha, "Detecting Copy move Forgery using DCT", International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013.

[7] Varsha Sharma, Swati Jha , Dr. Rajendra Kumar Bharti ,“Image Forgery and it’s Detection Technique: A Review,” 2016 International Research Journal of Engineering and Technology (IRJET), vol. 3,no.3,pp. 756-762

[8] Chihaoui, T., Bourouis, S., Hamrouni, K.: Copy-move image forgery detection based on sift descriptors and svd-matching. In: Advanced Technologies for Signal and Image Processing (ATSIP), 2014 1st International Conference on, pp. 125-129. IEEE (2014)

[9] Wang, Y.Y., Li, Z.M., Wang, L., Wang, M.: A scale invariant feature transform based method. Journal of Information Hiding and Multimedia Signal Processing 4(2), pp. 73-89 (2013)

[10] Ryu, S.J., Kirchner, M., Lee, M.J., Lee, H.K.: Rotation invariant localization of duplicated image regions based on zernike moments. IEEE Transactions on Information Forensics and Security 8(8), pp.1355-1370 (2013)

[11] Gavin Lynch, Frank Y.Shih and Hong-Yuan Mark Liao, "An efficient expanding block algorithm for image copy-move forgery detection", 0020-0255/$ -see front matter 2013 Elsevier Inc.

[12] Deepali N. Pande, A.R. Bhagat Patil and Antara S. Bhattacharya, "Generic Algorithm for Image Tampering Detection Based on Claimant Suspect Decision Rule", International Journal of Computer Science Engineering and Technology(IJCSET) | April 2014 | Vol 4, Issue 4,121- 124.

[13] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo and G. Serra, "A SIFT-Based Forensic Method for copy–Move Attack Detection and Transformation Recovery," in IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1099-1110, Sept. 2011.

[14] G. Muhammad, M. Hussain, K. Khawaji and G. Bebis, “Blind copy move image forgery detection using dyadic undecimated wavelet transform,” 17th International Conference on Digital Signal Processing (DSP), Corfu, 2011, pp. 1-6.

[15] B. Xu, G. Liu and Y. Dai, “A Fast Image Copy-Move Forgery Detection Method Using Phase Correlation,” Fourth International Conference on Multimedia Information Networking and Security, Nanjing, 2012, pp. 319- 322.

[16] V. Christlein, C. Riess, J. Jordan, C. Riess and E. Angelopoulou, “An Evaluation of Popular Copy-Move Forgery Detection Approaches,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pp.1841-1854, Dec. 2012.

[17] H. C. Nguyen and S. Katzenbeisser, “Detection of Copy-move Forgery in Digital Images Using Radon Transformation and Phase Correlation,” Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Piraeus, 2012, pp. 134-137.

[18] Le Zhong and Weihong Xu, “A robust image copy-move forgery detection based on mixed moments,” 4th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, 2013, pp.381-384.

[19] S. Kumar, J. Desai and S. Mukherjee, “A fast DCT based method for copy move forgery detection,” IEEE Second International Conference on Image Information Processing (ICIIP), 2013, Shimla, 2013, pp. 649-654.

[20] M. F. Hashmi, A. R. Hambarde and A. G. Keskar, “Copy move forgery detection using DWT and SIFT features,” 13th International Conference on Intellient Systems Design and Applications, Bangi, 2013, pp. 188-193.

[21] G. Muhammad, M. H. Al-Hammadi, M. Hussain, A. M. Mirza and G.Bebis, “Copy move image forgery detection method using steerable pyramid transform and texture descriptor,” IEEE EUROCON, 2013, Zagreb, 2013, pp. 1586-1592.

[22] S. Chakraborty, “Copy move image forgery detection using mutual information,” Fourth International Conference on Computing,

DOI : 10.35291/2454-9150.2019.0148

Communications and Networking Technologies (ICCCNT),2013, Tiruchengode, 2013, pp. 1-4.

[23] S. Ketenci and G. Ulutas, "Copy-move forgery detection in images via 2D-Fourier Transform," 36th International Conference on Telecommunications and Signal Processing (TSP), 2013, Rome, 2013, pp. 813-816.

[24] M. AlSawadi, G. Muhammad, M. Hussain and G. Bebis, "Copy-Move Image Forgery Detection Using Local Binary Pattern and Neighborhood Clustering," Modelling Symposium (EMS), 2013, pp. 249-254, European, Manchester, 2013.

[25] M. F. Hashmi, V. Anand and A. G. Keskar, "A copy-move image forgery detection based on speeded up robust feature transform and Wavelet Transforms," International Conference on Computer and Communication Technology (ICCCT), 2014, Allahabad, 2014, pp. 147-152.

[26] S. A. Fattah, M. M. I. Ullah, M. Ahmed, I. Ahmmed and C. Shahnaz, "A scheme for copy-move forgery detection in digital images based on 2D-DWT," IEEE 57th International Midwest Symposium on Circuits and Systems (MWSCAS), College Station, TX, 2014, pp. 801-804.

[27] S. M. Fadl, N. A. Semary and M. M. Hadhoud, "Copy-rotate-move forgery detection based on spatial domain," 9th International Conference on Computer Engineering and Systems (ICCES), Cairo, 2014, pp. 136-141.

[28] L. Yu, Q. Han and X. Niu, "Copy-Rotation-Move Forgery Detection Using the MROGH Descriptor," IEEE International Conference on Cloud Engineering (IC2E), 2014, Boston, MA, 2014, pp. 510-513.

[29] Ayalneh, D. A., Kim, H. J., & Choi, Y. S. (2014). JPEG copy paste forgery detection using BAG optimized for complex images. In International Conference on Advanced Communication Technology, ICACT (pp. 181-185). [6778945] Institute of Electrical and Electronics Engineers Inc.. https://doi.org/10.1109/ICACT.2014.6778945

[30] K. Sudhakar, V. M. Sandeep and S. Kulkarni, "Shape Based Copy Move Forgery Detection Using Level Set Approach," Fifth International Conference on Signal and Image Processing (ICSIP), 2014, Jeju Island, 2014, pp. 213-217.

[31] Kashyap, Abhishek; B. Suresh; Agrawal, Megha; Gupta, Hariom; Joshi, Shiv Dutt, "Detection of splicing forgery using wavelet decomposition," IEEE International Conference on Computing, Communication and Automation (ICCCA), Noida, 15-16 May 2015, pp. 843-848.

[32] Reddy Chandra Sharath K. and Dalal Tarun. "Novel approach for Image Forgery Detection Technique based on colour illumination using machine learning approach." International Journal of Advance Research, Ideas and Innovations in Technology, Volume-2, Issue-4, 2016

[33] Somayeh Sadeghi, Hamid A. Jalab, and Sajjad Dadkhah," Efficient Copy-Move Forgery Detection for Digital Images", World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering Vol:6, No:11, 2012

[34] Bo Xu, Guangjie Liu, and Yuewei Dai, The Scientific World Journal, Detecting Image Splicing Using Merged Features in Chroma Space, Volume 2014, Article ID 262356, 8 pages, http://dx.doi.org/10.1155/2014/262356

[35] Lovepreet Kaur, Raghuwinder Kaur and Simran Kaur. Forgery Detection Techniques: A Review. International Journal on Emerging Technologies (Special Issue on RTIESTM-2016) 7(1): 170-174(2016)

[36] P. Kakar and N. Sudha, "Exposing Postprocessed Copy–Paste Forgeries Through Transform-Invariant Features," in IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 1018-1028, June 2012.

[37] Minati mishra, Flt. Lt. Dr. M C. Adhikary, " Digital image tamper detection techniques- A comprehensive study", 2013

[38] Deepika Sharma , Pawanesh Abrol, Digital Image Tampering – A Threat to Security Management, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 10, October 2013

[39] M. T. H. Majumder and A. B. M. Alim Al Islam, "A Tale of a Deep Learning Approach to Image Forgery Detection," 2018 5th International Conference on Networking, Systems and Security (NSysS), Dhaka, Bangladesh,2018,pp.1-9.

[40] N.Anantharaj "Tampering and Copy move forgery detection using shift Feature", International Journal of Innovative Research in Computer and Communication Engineering,Vol.2, Special Issue 1, March 2014

[41] Yongzhen Ke Weidong Min Fan Qin Junjun Shang "Image Forgery Detection Based on Semantic" International Journal of Hybrid Information Technology vol. 7 no. 1 pp. 109-124 2014

[42] https://timesofindia.indiatimes.com/city/kolkata/seven-held-in-cheque-fraud-racket-bust-stolen-amount-may-run-into-crores/articleshowprint/66930289.cms

[43] 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. doi: 10.1109/ICIP.2014.7026075

[44] Arun Anoop M, "Image forgery and its detection: A survey," 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2015, pp. 1-9. doi: 10.1109/ICIIECS.2015.7193253

[45] Siddhi Gaur, Shamik Tiwari, Image Splicing Forgery Detection, Proceedings of International Conference on Recent Innovations in Engineering and Technology, Jaipur, India, 18th - 19th Feb'2017, ISBN: 978-93-86291-63-9

[46] Gjomemo, R., Malik, H., Sumb, N., Venkatakrishnan, V. N., & Ansari, R. (2014, March). Digital check forgery attacks on client check truncation systems. In International conference on financial cryptography and data security (pp. 3–20). Springer, Berlin, Heidelberg.

[47] Maloth Rajender, Rajarshi Pal "Detection of Manipulated Cheque Images in Cheque Truncation System Using Mismatch in Pixels, "2nd International Conference on Business and Intonation Management (lCBIM), 2014

[48] https://www.pocket-lint.com/apps/news/adobe/140252-30-famous-photoshopped-and-doctored-images-from-across-the-ages

[49] Chhabra, S., Gupta, G., Gupta, M., & Gupta, G. (2017). Detecting Fraudulent Bank Checks. IFIP Advances in Information and Communication Technology, 245–266.doi:10.1007/978-3-319-67208-3_14

[50] Parveen, A., Khan, Z. H., & Ahmad, S. N. (2019). Block-based copy–move image forgery detection using DCT. Iran Journal of Computer Science.doi:10.1007/s42044-019-00029-y

[51] A. Kashyap, R. S. Parmar, B. Suresh, M. Agarwal and H. Gupta, "Detection of digital image forgery using wavelet decomposition and outline analysis," 2016 International Conference on Signal Processing and Communication (ICSC), Noida, 2016, pp. 187-190.

[52] "Detecting Splicing and Copy-Move Attacks in Color Images," 2018 Digital Image Computing: Techniques and Applications (DICTA), Canberra, Australia, 2018, pp. 1-7.

[53] Dixit, R., & Naskar, R. (2017). Review, analysis and parameterisation of techniques for copy–move forgery detection in digital images . IET Image Processing, 11(9), 746–759.doi:10.1049/iet-ipr.2016.0322

[54] Teddy Surya Gunawan, Siti Amalina Mohammad Hanafiah, Mira Kartiwi, Nanang Ismail, Nor Farahidah Za'bah, Anis Nurashikin Nordin, "Development of Photo Forensics Algorithm by Detecting Photoshop Manipulation Using Error Level Analysis" Indonesian Journal of Electrical Engineering and Computer Science Vol. 7, No. 1, July 2017, pp. 131 ~ 137

[55] Basavarajappa, Shwetha B & Sathyanarayana, S. (2016). Digital image forgery detection techniques: a survey. ACCENTS Transactions on Information Security. 2. 22-31. 10.19101/TIS.2017.25003.

[56] T. Mahmood, T. Nawaz, Z. Mehmood, Z. Khan, M. Shah and R. Ashraf, "Forensic analysis of copy-move forgery in digital images using the stationary wavelets," 2016 Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, 2016, pp. 578-583.

[57] G. Nirmala and K. K. Thyagharajan, "A Modern Approach for Image Forgery Detection using BRICH Clustering based on Normalised Mean and Standard Deviation," 2019 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2019, pp. 0441-0444.

[58] C. Pasquini, G. Boato and R. Bohme, "Teaching Digital Signal Processing With a Challenge on Image Forensics [SP Education]," in IEEE Signal Processing Magazine, vol. 36, no. 2, pp. 101-109, March 2019.

[59] M. N. Nazli and A. Y. A. Maghari, "Comparison between image forgery detection algorithms," 2017 8th International Conference on Information Technology (ICIT), Amman, 2017, pp. 442-445.

DOI : 10.35291/2454-9150.2019.0148

[60] S. Ranjan, P. Garhwal, A. Bhan, M. Arora and A. Mehra, "Framework for Image Forgery Detection and Classification Using Machine Learning," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, 2018, pp. 1-9. doi: 10.1109/ICOEI.2018.8553924

[61] Anil Dada Warbhea, R. V. Dharaskar, V. M. Thakare, A Survey on Keypoint Based Copy-Paste Forgery Detection Techniques, Procedia Computer Science 78 (2016) 61 – 67

[62] H. Huang, W. Guo, Y. Zhang, Detection Of Copy-Move Forgery in Digital Images Using SIFT Algorithm, in: IEEE Pacific-Asia Work. Comput. Intell. Ind. Appl., Ieee, 2008: pp. 272–276. doi:10.1109/PACIIA.2008.240.

[63] https://en.wikipedia.org/wiki/Cheque_Truncation_System

[64] Ashish Kumar Chakraverti, Prof.(Dr.) Vijay Dhir, A Review on Image Forgery & its Detection Procedure IJARCS All Rights Reserved, Volume 8, No. 4, May 2017 (Special Issue)

[65] Navneet Kaur, Navdeep Kanwal, "Review And Analysis of Image Forgery Detection Technique for Digital Images",International Journal of Advanced Research in Computer Science, Volume 8, No. 5, May – June 2017

[66] N. K. Gill, R. Garg and E. A. Doegar, "A review paper on digital image forgery detection techniques," *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Delhi, 2017, pp. 1-7.

[67] Jyoti A. Yadav, Nilima Dongre, Analysis of Copy-Move Forgery Detection in Digital Image 2017 International Journal of Engineering Development and Research, Volume 5, Issue ISSN: 2321-9939

[68] http://listverse.com/2007/10/19/top-15-manipulated-photographs/

[69] https://www.cc.gatech.edu/~beki/cs4001/history.pdf

[70] Nisha, Kansal Rajnish,Classification of Copy Move Forgery and Normal Images by ORB Features and SVM Classifier, International Journal of Advance Research, Ideas and Innovations in Technology,(Volume3, Issue2), 2017

[71] Chhaya Saini,Priya Singh,Pramod Kr. Sethy,Raj Kumar Saini,Digital Image Forgery Detection using Correlation Coeficients, International Journal of Computer Applications (0975 – 8887),Volume 129 – No.14, November2015

[72] https://www.cnet.com/pictures/pictures-that-lie-photos/8/

[73] http://pth.izitru.com/2010_06_00.html

[74] C.Rajalakshmi, Dr.M.Germanus Alex, Dr. R. Balasubramanian , Study Of Image Tampering And Review Of Tampering Detection Techniques, International Journal of Advanced Research in Computer Science, Volume 8, No. 7, July – August 2017,ISSN No. 0976-5697

[75] Long, Fei, "Digital image forensics" (2011). Theses. 91. https://digitalcommons.njit.edu/theses/91

[76] Gill, N. K., Garg, R., & Doegar, E. A. (2017). A review paper on digital image forgery detection techniques. 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT).

[77] https://blog.filestack.com/api/copy-move-forgery-detection/

[78] https://gizmodo.com/29-viral-photos-and-gifs-from-2017-that-were-totally-fa-1821440079

[79] https://www.snopes.com/fact-check/marilyn-monroe-liz-taylor/

[80] https://www.ijedr.org/papers/IJEDR1701116.pdf

[81] isis.poly.edu/~forensics/pubs/copymovesurvey.pdf

[82] Neetu Yadav and Rupal Kapdi. Copy Move Forgery Detection Using SIFT Features- An Analysis. Nirma University Journal Of Engineering And Technology, Vol. 4, No. 1, Jan-Jun 2015

[83] https://www.currenttrending.com/cheque-truncation-system/

[84] Soni, B., Das, P. K., & Thounaojam, D. M. (2018). CMFD: a detailed review of block based and key feature based techniques in image copy-move forgery detection . IET Image Processing, 12(2), 167–178. doi:10.1049/iet-ipr.2017.0441

[85] Salam A.Thajeel ,Ghazali Bin Sulong,State Of The Art Of Copy-Move Forgery Detection Techniques: A Review,Ijcsi International Journal of Computer Science Issues, Vol. 10, Issue 6, No 2, November 2013 ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784 www.IJCSI.org

[86] Ketenci, S., & Ulutas, G. (2013). Copy-move forgery detection in images via 2D-Fourier Transform. 2013 36th International Conference on Telecommunications and Signal Processing (TSP).doi:10.1109/tsp.2013.6614051

[87] Dhivya, S & B, Sudhakar. (2018). A Scrutiny on Copy Move Forgery Detection Using Novel Methods.

[88] Pradyumna Deshpande , Prashasti Kanikar. Pixel Based Digital Image Forgery Detection Techniques. International Journal of Engineering Research and Applications (IJERA)Vol. 2, Issue 3, May-Jun 2012, pp. 539-543

[89] Prinkle Rani,Er. Jyoti Rani. Copy-Move Forgery Attack Detection in Digital Images .International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181 Vol. 4 Issue 06, June-2015

[90] Soni, Badal & Das, Pradip & Thounaojam, Dalton. (2018). multiCMFD: fast and efficient system for multiple copy-move forgeries detection in image. 53-58. 10.1145/3191442.3191465.

[91] R, Cristin & Cyril Raj, Velankanni. (2017). Consistency features and fuzzy-based segmentation for shadow and reflection detection in digital image forgery. Science China Information Sciences. 60. 10.1007/s11432-016-0478-y.

[92] Wu, Yue & Abd-Almageed, Wael & Natarajan, Prem. (2018). BusterNet: Detecting Copy-Move Image Forgery with Source/Target Localization: 15th European Conference, Munich, Germany, September 8–14, 2018, Proceedings, Part VI. 10.1007/978-3-030-01231-1_11.

[93] Mahmood, T., Nawaz, T., Irtaza, A., Ashraf, R., Shah, M., & Mahmood, M. T. (2016). Copy-Move Forgery Detection Technique for Forensic Analysis in Digital Images. Mathematical Problems in Engineering, 2016, 1–13.doi:10.1155/2016/8713202

[94] Aymaz, Samet & Aymaz, şeyma & Ulutas, Guzin. (2016).Detection of copy move forgery using Legendre Moments. 1125-1128. 10.1109/SIU.2016.7495942.

[95] Navpreet Kaur Gill , Ruhi Garg , Amit Doegar. “A Hybrid Technique For Copy-Move Forgery Detection In Digital Images”. International Journal of Advance Research in Science and Engineering. Vol.No.6,Issue No. 08, August 2017

[96] Harpreet Kaur and Sheenam Malhotra. Review on Block Based Copy Move Image Forgery Detection Techniques. International Journal of Advance Research in Computer Science and Management Studies, Volume 4, Issue 2, February 2016

[97] Panda S., Mishra M. (2018) Passive Techniques of Digital Image Forgery Detection: Developments and Challenges. In: Kalam A., Das S., Sharma K. (eds) Advances in Electronics, Communication and Computing. Lecture Notes in Electrical Engineering, vol 443. Springer, Singapore

[98] Niyishaka P., Bhagvati C. (2018) Digital Image Forensics Technique for Copy-Move Forgery Detection Using DoG and ORB. In: Chmielewski L., Kozera R., Orłowski A., Wojciechowski K., Bruckstein A., Petkov N. (eds) Computer Vision and Graphics. ICCVG 2018. Lecture Notes in Computer Science, vol 11114. Springer, Cham

[99] Bappy, Md Jawadul & Simons, Cody & Nataraj, Lakshmanan & Manjunath, B & Roy-Chowdhury, Amit. (2019). Hybrid LSTM and Encoder-Decoder Architecture for Detection of Image Forgeries.

[100] Misbah U.Mulla and Prabhu R.Bevinamarad. Review of Image Splicing Forgeries. International Journal of New Innovations in Engineering and Technology (2017)

[101] https://reviews.pribome.com/2019/03/08/famous-photoshopped-and-doctored-images-from-across-the-ages/

[102] https://businessjargons.com/cheque-truncation-system.html

DOI : 10.35291/2454-9150.2019.0148