Volume 4 Issue IX, September 2016
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A literature review of Image Forgery Detection

Er.Isha[1], Er.Vikas Goyal[2]
[1] Research Scholar, [2] Assistant Professor
Department of Electronics and Communication Engineering, Panipat Institute of Engineering and Technology, Samalkha, Panipat

Abstract--The utilization of advanced pictures has expanded in the course of recent years to spread a message. This expands the need of picture authentication. But Preserving picture genuineness is exceptionally mind boggling on the grounds that effortlessly accessibility of picture altering programming. The pixel-based picture imitation identification intends to confirm the legitimacy of advanced pictures with no earlier learning of the first picture. There are numerous routes for altering a picture, for example, joining or copy move, re-examining a picture (resize, pivot and stretch), addition and expulsion of any item from the picture. Copy move falsification is a standout amongst the most prevalent altering ancient rarities in computerized pictures. In this paper we display diverse strategy to distinguish copy move imitation utilizing piece based technique.

Keywords: Image processing, Image forensic, Forgery detection, Watermarking, Digital signature.

I. INTRODUCTION

Computerized Image Forensics is a developing branch of picture handling. Advanced Image Forensics is that field which manages the validations of the pictures. Computerized picture forensics checks the uprightness of the pictures by identifying different forgeries [1].One of the key errands of picture forensics is picture forgery identification. Altering intends to meddle with something keeping in mind the end goal to bring about harm or make unapproved alterations [2].The accessibility of ease equipment and programming devices, makes it simple to make, modify, and controlled advanced pictures with no undeniable clues[6].Such programming can do an adjustment in computerized picture by changing squares of a picture without demonstrating the impact of the alteration in the produced picture. These changes can't be seen by human eye [8].It might never again be conceivable to recognize whether a given advanced pictures is unique or an adjusted variant. Computerized picture forgery is a developing issue in criminal cases and in broad daylight course. Distinguishing forgery in computerized pictures is a rising exploration field for guaranteeing the validity of advanced pictures .In the later past advanced picture control could be found in newspaper magazine, design industry, scientific journals, court rooms, fundamental media outlet and photograph tricks we get in our email[3].

A. Applications of Digital Image Forensic

1) Digital forensics is commonly used in both criminal law and private investigation.

2) Forensic analysis if images on online social networks.

3) Used for detecting tampered or forged images.

4) Image forgery detection system is needed in many fields for protecting copyright and preventing Forgery or alteration of images. It is applied in areas such as journalism, scientific publications, digital forensic science, multimedia security, surveillance systems etc.

B. Classifications of Approaches

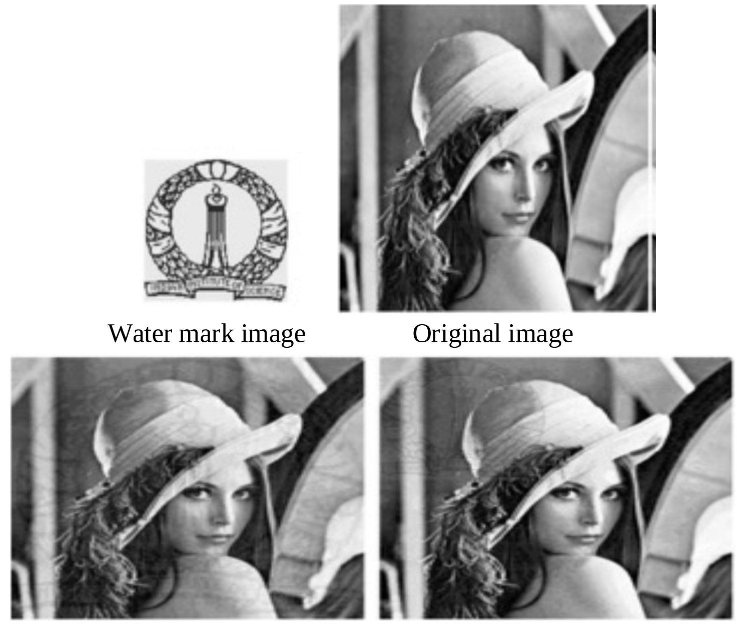
Computerized picture forgery discovery methods are ordered into dynamic and aloof approach.

C. Dynamic Approaches

A dynamic location technique which comprises of adding picture points of interest so as to depict computerized altering, for example name, date, signature, etc [22]. It requires an extraordinary equipment execution to check the verification of the computerized picture.

D. Techniques of Active Approach

1) *Watermarking*--Watermarking is used for image forgery detection .Watermark must be embedded at the season of making the picture. Installing a watermark in the picture/video is proportionate to marking a particular computerized maker distinguishing proof (mark) on the substance of pictures/recordings. Once the picture/video is controlled, this watermark will be devastated such that the authenticator can look at it to confirm the innovation of contents. The watermarking comprises of concealing an imprint or a message in a photo keeping in mind the end goal to secure its copyright at the season of picture obtaining and to check the legitimacy this message is separated from the picture and confirmed with the first watermarks. In the event that picture is not controlled these watermarks will stay same else they won't coordinate the first watermarks. Thus this strategy depends on the source data before hand. Some camera sources don't insert watermarks into picture consequently this technique is not that helpful and more often than does not function admirably with lossy compression [32].


Water mark image Original image

Watermarked original image
(Watermark over the whole image)

Watermarked original image
(Watermark at the corner)

Fig1 Example of Watermarking

2) *Digital Signatures:* Advanced mark is some kind of cryptographic is a scientific plan for exhibiting the validness of computerized document[6].It creates a substance based computerized signature which incorporates the essential data of substance and the selective maker recognizable proof .The mark is produced by a maker particular private key such that it cannot be manufactured. In this manner, the authenticator can check a got picture/video by inspecting whether its substance coordinate the data passed on in the mark.

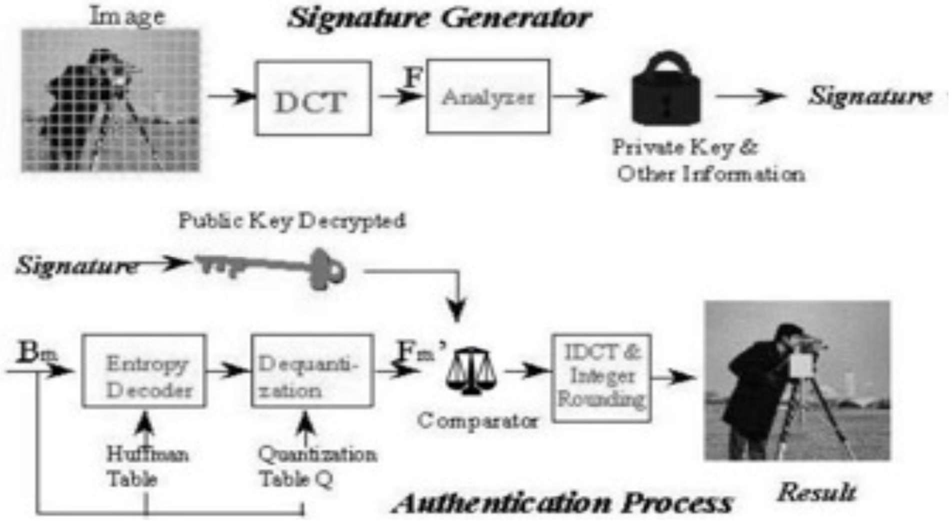


Fig2 Signature Generator and Image Authentication Process

A mark and a picture are produced in the meantime. The mark is an encoded type of the element codes or hashes of this picture, and it is put away independently. Once a client needs to verify the picture he gets, he should decrypt this mark and think about the component codes (or hash qualities) of this picture to their relating values in the first signature. On the off chance that they coordinate, this picture can be guaranteed to be "authentic"[31].

3) *Advantage of Active Approach:*
Computational cost less, simple if knowledge about original image is available.

4) *Disadvantage of Active Approach*
a) These techniques require prior knowledge about original image thus they are not automatic. They required some human intervention or specially equipped cameras.
b) There are more than millions of digital images on internet without digital signature or watermark. In such scenario active approach could not be used to find the authenticity of the image [7].
c) In Digital Signature scheme, extra bandwidth is needed for transmission of Signature.

5) *Passive Approach:* Latent strategy distinguishes the copied objects in manufactured pictures without need of unique picture watermark and relies upon follows left on the picture by various preparing ventures amid picture control. Uninvolved approach likewise decides the some of the area of fraud in the picture. There are two strategies for inactive methodology**.**Picture source ID-It distinguishes the gadget utilized for the securing of the advanced picture. It tells that the picture is PC produced or advanced camera picture. In this technique the area of imitation in picture can't be resolved.Altering recognition-It recognizes the deliberate control of pictures for malignant purposes. Picture control is meant as altering when it goes for adjusting the substance of the visual message [32].
a) *Techniques of Passive Approach*
1. Pixel-based techniques that detect statistical anomalies introduced at the pixel level.
2. Format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme.
3. Camera-based techniques that exploit artifacts introduced by the camera lens, sensor, or on-chip post-processing.
4. Physically based techniques that explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light, and the camera.
5. Geometric-based techniques that make measurements of objects in the world and their positions relative to the camera [5].

b) *Advantage of passive approach:* Pre existing digital images and data cannot gain any profit using Active approach. Passive approach overcomes this disadvantage that the pre-existing images can also be catered using this approach.
c) *Disadvantage of passive approach:* These techniques based on the assumption that digital forgeries may leave no visual clues that indicate tampering, so they require different statistics of an image. Thus it is complex.

6) *Types of Digital Image Forgery:* The forgeries are classified into five major categories
a) Image Retouching
b) Image Splicing
c) Copy-Move (cloning)
d) Morphing
e) Enhanced

Picture Retouching-- where the strategy is utilized for improves a picture or decreases some component of a picture and upgrades the picture quality for catching the pursuer’s consideration. In this technique, the expert picture editors change the foundation, fill some appealing hues, and work with tint immersion for conditioning and adjusting.
Picture Splicing--where the diverse components from different pictures are consolidated in a solitary. Such grafting can more often than not be identified via looking the joining limit (or the impact of the grafting on picture measurements).
Copy Move--in the copy move, a part of the picture is replicated and stuck elsewhere inside the same picture. This strategy more often than not for cover up clear particulars or to coordinating persuaded highlights regarding a picture .The obscure apparatus is use for modifying outskirts and lessening the impact amongst unique and glued region [23]

II. COPY-MOVE FORGERY DETECTION

Copy Move picture fabrication is the generally utilized strategy to alter the computerized image. Copy-Move phony is performed with the goal to make an item "vanish" from the picture by covering it with a little square replicated from another part of the same picture. Since the replicated portions originate from the same picture, the shading palette, clamor segments, shading and alternate properties will be same with whatever remains of the picture, in this manner it is extremely troublesome for a human eye to detect[3].A copy move fraud is anything but difficult to make. The copied substance of picture which is utilized to perform fraud is called scrap. As the source and the objective areas are from the same picture, the picture highlights like commotion, shading, and enlightenment condition and so on will be same for the manufactured locale and whatever is left of the picture. A sharp counterfeiter may likewise do some post-handling on the copied area like pivot, scaling, obscuring, commotion expansion before the locale is stuck. These elements make the fraud location more mind boggling. So the significant point in such a phony identification procedure would be extraction of features [2].

By and large, Copy-Move fabrication discovery strategies can be arranged into two: Block based methodologies and Keypoint based methodologies [7].In both the methodologies some type of pre-handling will be there. Unlike piece based techniques, Keypoint based strategies figure their elements just on picture locales with high entropy, with no picture subdivision for don't separate the picture into squares to extricate the components rather than the elements are removed from the entire image. There are two sorts of keypoint based strategies, for example, Scale Invariant Feature Transform (SIFT) and Speeded up Robust Features (SURF). Piece based strategies subdivide the picture into covering squares of indicated size for highlight extraction. Comparable component vectors are in this manner coordinated. There are 13 square based elements and it can be gathered into four classes: Moment-based (Blur[13], Hu, Zernike[12]), Dimensionality decrease based (PCA[5],SVD[11], KPCA), Intensity-based (Luo [10],Lin, Bravo, Circle[14]), Frequency - based (DCT[8][9], DWT, FMT[12]).

III. COMPARISON BETWEEN EXISTING TECHNIQUES

S. No	Author/Year	Methodology	Advantage	Disadvantage
1	J. Fridrich, 2003[8]	DCT	Copy-move region is detected	Will not work in noisy image
2	Popescu, 2004[9]	PCA	Efficient method, low false positives	Low efficiency for low quality of image, low SNR and small blocks
3	W. Q. Lou, 2006[10]	Similarity matching	Copy-move region is detected in noisy conditions	Time complexity is reduced
4	G. H. Li, 2007	DWT-SVD	Efficiently detects Forged region	Time complexity is less compared to other algorithms
5	Mahdian, 2007[13]	BLUR	Copied region detect with changed contrast values and blurred regions can also be detected	High computation time of the algorithm
6	J. Zhang, 2008	DWT	Exact copy-move region is detected	Works well in noisy and compressed image
7	H. Huang, 2008	SIFT	Copy-move region is detected	Detects false result also
8	X. Kang, 2008	SVD	Copy-move region is detect accurately	Will not work in highly noised & compressed image
9	Wang, 2009	CIRCLE	Working for post-processing like blurring, rotating, noise adding etc	Scaling and geometric transformations cannot be detected
10	H.J. Lin 2009	Improved PCA	Exact copy-move region is detected ,works well in noisy	Not accurate

11	Z. Lin 2009	Double Quantization DCT	Tampered region is detected accurately	Works only in JPEG format
12	Ting, 2009	SVD	Can detect duplication even post processing is done, robust and computationally less complex	Cannot detect copy paste regions
13	Bayram, 2009[12]	FMT	Efficient and robust to blurring, noise, scaling, lossy, JPEG compression and translation effects	Cannot detect forgeries which have rotation of above 10deg and scaling
14	Wang, 2009	HU	Robust and efficient method, detects post-processing effects like noise addition, blurring, lossy compression etc	Many false positives
15	Qiao, 2011	CURVELET	Multi-dimensional and multidirectional gives precise results	Cannot be applied on compressed images
16	M. Ghorbani, 2011	DCT-DWT	Forged region is detected	Will not work in highly compressed image
17	S. D. Lin, 2011	DCT-SURF	Copy-move and spliced both region detected	Not accurate
18	Muhammad, 2012	DWT	Reduced false positives .Advantageous than previous methods	Tested only for small rotation angle and good quality images
19	Cao Y, 2012	Circular block with DCT	Perfect detection for uniform background images, non regular copy regions, high resolution images.	Poor performance with poor image quality. Not robust to geometrical operations
20	L. Gavin, 2013	Expanding blocks	Detection with irregularly shaped regions and for forged regions slightly darkened or lightened	Slow in execution. Number of false positives more when compared to other methodology
21	Mohamdian, 2013 [28]	ZERNIKE	Flat regions of forgeries are detected	Calculating Zernike moment coefficients is complex
22	Zhong L, 2013	Mixed moments	Tested for rotation, scaling, brightness enhancement contrast changes reduce number	Qualitative evaluation not specified Rotation angle and scaling factor not specified.
23	Zhu H, 2013	Polar harmonic transform	Addressed affine transforms like shearing and perspective projections	Simulation result always

IV. CONCLUSION

Copy Move imitation location in advanced pictures is more pervasive issue amid the previous a few decades. Numerous procedures have been proposed to address this issue. This paper provides brief study to identify copy move fraud identification strategy. This likewise covers restrictions of various systems utilized for aloof strategy to identify copy move fabrication. The near work can be stretched out by proposing a novel strategy with which the current constraints can be overcome.

REFERENCES

[1] Mohd Dilshad Ansari, S. P.Ghera & Vipin Tyagi: "Pixel-Based Image Forgery Detection: A Review", IEEE Journal of Education, 40-46, Aug 2014.

[2] Resmi Sekhar, ChithraAS: "Recent Block-based Methods of Copy-Move Forgery Detection in Digital Images", International Journal of Computer Applications (0975 – 8887), Volume 89, no. 8, March 2014.

[3] Rohini.A.Maind, Alka Khade, D.K.Chitre:"Image Copy Move Forgery Detection using Block Representing Method" International Journal of Soft Computing and Engineering (IJSCE)ISSN: 2231-2307, Volume-4, Issue-2, May 2014.

[4] Ms. P. G.Gomase, Ms. N. R. Wankhade: "Advanced Digital Image Forgery Detection: A Review Journal of Computer Science (IOSR-JCE) e-ISSN: 2278-0661, PP 80-83.

[5] Hany Farid: "Image Forgery Detection", IEEE Signal Processing Magazine, pp. 16-25, March 2009.

[6] Nikhil Kumar, P. Joglekar, Dr.P.N. Chatur: "A Compressive Survey on Active and Passive Methods for Image Forgery Detection: "International Journal Of Engineering And Computer Science ISSN: 2319-7242,Volume 4, Page No. 10187-10190, 1 January 2015.

[7] Dr. S.D. Chede, Prof. P.R.Lakhe:"Forgery of Copy Move Image Detection Technique by Integrating Block and Feature Based Method", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 1, January 2015.

[8] J. Fridrich, D. Soukalm and J. Lukas: "Detection of Copy-Move Forgery in Digital Images" Digital Forensic Research Workshop, Cleveland, 2003.

[9] A.C.Popescu and H.Farid: "Exposing Digital Forgeries by Detecting Copied Image Regions", Tech.Rep.TR2004-515, Dartmouth College, 2004.

[10] W. Luo, J. Huang and G. Qiu, "Robust detection of region-duplication forgery in digital images", International Conference on Pattern Recognition, vol. 4, 2006.

[11] X.Kang and S.Wei, "Identifying tampered regions using singular value decomposition in digital image forensics", Proceedings of International Conference on Computer Science and Software Engineering, 2008.

[12] S.Bayram, H.T.Sencar and N.Memon, "An efficient and robust method for detecting copy-move forgery", IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE Press, New York 2009.

[13] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants", Forensic Sci. Int., vol. 171, (2007) pp. 180–189.

[14] L. Li, S. Li, H. Zhu, S.-C. Chu, J. F. Roddick, and J.-S. Pan, "An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns", Journal of Information Hiding and Multimedia Signal Processing vol. 4, no. 1, (2013) January, pp. 46-56.

[15] G. Lynch, F.Y. Shih and H. M. Liao, "An efficient expanding block algorithm for image copy-move forgery detection", Inf. Sci., vol. 239, (2013), pp. 253–265.

[16] Li L, Li S, Zhu H, Wu X. "Detecting copy-move forgery under affine transforms for image forensics", Computer Electric Eng (2013)

[17] Cheng Yan: "Research on Forged Identification of Forged Images", International Conference on Mehatronic Sciences, Electric Engineering and Computer,20 Dec 2013.

[18] Ashima Gupta, Nisheeth Saxena, S.K Vasisth: "Detecting Copy Move Forgery Using DCT", International Journal of Scientific and Research Publication, Vol.3, Issue5, May 2013.

[19] Amanpreet Kaur, Richa Sharma: "Optimization of Copy-Move Forgery Detection Technique", International Journal of Advanced Research in Computer Science and Software Engineering Vol 3, Issue 4, April 2013.

[20] Wei Hou, ZheJi, Xin Jin, Xing Li :"Double JPEG Compression Detection Based on Extended First Digit Features of DCT Coefficients", International Journal of Information and Education Technology, Vol. 3, No. 5,October 2013.

[21] Abhitha.E, V.J Arul Karthick: "Forensic Technique for Detecting Tamper in Digital Image Compression", International Journal of Advanced Research in Computer and Communication EngineeringVol.2, Issue3, March2013.

[22] Salam A.Thajeel and Ghazali Bin Sulong: "State Of The Art Of Copy-Move Forgery Detection Techniques: A Review ", International Journal of Computer Science Issues, Vol. 10, Issue 6, No 2, November 2013.

[23] H. shah, P. Shinde and J. Kukreja: "Retouching detection and steg analysis", IJEIR, vol. 2, pp. 487-490, 2013.

[24] Salam A.Thajeel, Ghazali Bin Sulong: "A Survey of Copy-Move Forgery Detection Techniques", Journal of Theoretical and Applied Information Technology. Vol.70, 10thDecember 2014.

[25] Mariam Saleem: "A Key-Point Based Robust Algorithm for Detecting Cloning Forgery", International Journal of Current Engineering and Technology, Vol.4, No.4 (Aug 2014).

[26] M. Sridevi, C. Mala and S. Sandeep: "Copy-Move Image Forgery Detection in A ParallelEnvironment",2012.

[27] J. Fridrich, D. Soukal, and J. Lukas: "Detection of copy move forgery in digital images," in Proceedings of the Digital Forensic Research Workshop, Aug. 2003, pp. 5-8.

[28] Muhammad, G., Hussein, M. Bebis, G: "Passive copy move image forgery detection using undecimated dyadic wavelet transform", Digital Investigation (9), 2012.

[29] Cao Y, Gao T, Fan L, Yang Q: "A robust detection algorithm for copy-move forgery in digital images", Forensic Sci Int. 2012 Jan.

[30] Zhong L, Xu W: "A robust image copy-move forgery detection based on mixed moments", IEEE International Conference on Software Engineering and Service Sciences (ICSESS), May 2013.

[31] L Gavin, S Frank, L Hong-Yuan Mark: "An efficient expanding block algorithm for image copy-move forgery detection", Information Sciences 239, 2013.

[32] Amanpreet Kaur, Richa Sharma: "Copy-Move Forgery Detection using DCT and SIFT", International Journal of Computer Applications (0975 – 8887) Volume 70– No.7, May 2013.

[33] A Project Report on Watermarking of Digital Images by Saraju Prasad Mohanty.