ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 8, Issue 7, July 2021

Analysis of Various Image Blind Detection Techniques: Review

[1] Kanika, [2] Dr. Vivek Thapar, [3] Er. Gurjit Kaur
[1] Student, GNDEC, Ludhiana, India.
[2] [3] Assistant Professor, GNDEC, Ludhiana, India

Abstract: The computer algorithms are utilized in DIP to process the digital image. At present, digital image is one of the most important carriers helping people to obtain enormous volume of information. Indeed, an image equals immeasurable word. Copy move forgery is usually done to hide facts. For example, CMF hides, repeats, or moves the object in the image. It can visually conceal duplicate field components such as colour and light by copying it from the same image. In this review paper, various techniques of image blind detection are reviewed in terms of certain parameters.

Keywords: Image Blind, CMF, Keypoint matching, Classification

I. INTRODUCTION

Image processing comes under the family of signal processing. This approach takes the input in form of image and provides the output as an image or a group of attributes regarding the input image. Image processing is considered as an integral discipline of electrical engineering and computer science. Various image processing methods consider the images as 2-D signals and they make the implementation of existing signal processing methods to these images. Thus, the image processing is often recognized as the DIP (Digital Image Processing). But, a few other kinds of image processing schemes are also available like optical and analogue. The computer algorithms are utilized in DIP to process the digital image [1]. At present, digital image is one of the most important carriers helping people to obtain enormous volume of information. Indeed, an image equals immeasurable word. This means that there is tremendous information included in the images. The most common methods for image manipulation are digital image frauds, blurriness, and composition. Digital image forensics has become an important are of research for its applications in validity or detecting forged digital imagery. The objective of digital image forensic studies is to authenticate the validity of digital images and to discover the tampering functions implemented to them by retrieving every information concerning their past. The rapidly growing devices to acquire digital images (such as digital cameras, scanners etc.) have spread the digital images throughout the world. Now, users with the help of cost-free or inexpensive computer tool like paint, photoshop, Picasa can manipulate digital images effortlessly [7]. This results in the manipulation of numerous images, specifically composite forged images which are being appeared in many domains, for example, legal proof, political actions, technical experimentation, educational research, and newspapers. Digital forgery is an operation generally applied to eradicate visible signs of tampering that naked eye can notice. Therefore, there is the need of some algorithms to validate digital images and to detect manipulated images. Fraudsters usually apply two means to perform image forgery, i.e., copy move and splicing. The splicing aims to cover some unnecessary part in the same image by copying a part of a picture and later pasting it over other parts. Verifying discrepancies of certain properties, values, or attributes within the target image are the main steps involved in the detection of a spliced picture. Copy-move refers to a robust form of forgery. Copy move forgery is usually done to hide facts. For example, CMF hides, repeats or moves the object in the image. It can visually conceal duplicate field components such as color and light by copying it from the same image [8]. There are several factors that must be considered while developing a copy-move forgery detection (CMFD) method. First of all, CMFD must be able to provide highly accurate and reliable detection results. However, the developed technique is also required to be effective in the context of speed and computational intricacy in real-time. Therefore, at present, it is quite challenging to provide solution to the problems concerning speed-

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 8, Issue 7, July 2021

accuracy trade-offs. In addition, a competent copy move forgery detection method must be strong against a variety of attacks and tempering schemes.

The steps included in the above structure are discussed below:

a. Pre-processing: This is the initial phase that makes the execution of some conversion, transform or decomposition methods [9]. The pre-processing phase focuses on preparing and revealing the data in a way using which the subsequent feature extraction phase becomes more effective. The most simple and imperative techniques of pre-processing are grayscale conversion that are implemented to transform the RGB pixels into a grayscale image from a range of 0 to 255 and the RGB image is converted to HSV using colour space conversion. This phase also comprises the decomposition methods known as wavelet decomposition or PCA.

b. Feature Extraction: This phase is executed later on. Feature extraction is the most crucial phase assists in determining the entire accuracy of the system. A set of short but significant data vectors is generated for exposing every portion of the destination digital image. This step aims to generate feature descriptors from each block or keypoint achieved from earlier methods. These descriptors refer to vectors obtained from image data, which have a high degree of discriminatory strength. Thus, the original and the duplicated image in copy move forgery is required to produce a group of feature descriptors that is analogous or almost associated with each other. Each descriptor generated by a powerful extraction method will be highly discriminative in nature which will ultimately be depicted in the total accuracy of the detection framework.

c. Feature matching: This phase includes the discovery of similar feature vectors. For constraining the range of same feature vectors, sorting algorithm are applied to make the similar attributes adjacent and sorted in lexicographical and radix manner [12]. Moreover, the process to investigate the similar feature vectors is enhanced using locality-sensitive hashing (LSH). Several techniques are available for quantifying the similarity among the feature vectors like Euclidean distance and Manhattan distance

d. Localization and post-processing: This is the last phase in which filtering and processing of raw matched detection results was carried out for improving and generating the final detection results with the highest quality [15]. In case, the regions that the feature matching determined are represented in the map, various isolated points and morphologic operations, filtering or random sample consensus (RANSAC) algorithm are implemented for the refinement of detected regions.

2. LITERATURE REVIEW

TinggeZhul, et.al (2019) presented a forgery detection technique on the basis of LBP residue classes and color regions [21]. The partition of an image was done into overlapped blocks. The evaluation of LBP residue classes was performed for every block. The plane generated through 'a' dimensional and 'b' dimensional from Lab color space was split into sixteen regions. The similar LBP residue class and color region had employed to investigate the same blocks and their grouping was performed into various regions later on. At last, the tampered areas were located by analyzing the multi-region relation of these suspicious regions and their areas. The experimental outcomes exhibited that the presented technique performed efficiently in enhancing the DR and mitigating the execution time even under different challenging conditions. This technique had potential to decrease the search range for same blocks. Thus, it provided the greater speed as compared to exhaustive search and comparative detection results simultaneously.

Navdeep Kanwal, et.al (2019) discussed that the methods of forgery detection executed into 2 domains of image forgery: CMFD and ISD [22]. A detailed comparative analysis was carried out to make the utilization of local texture descriptors such as LBP and LTP in detecting the forgery of an image. A method was also put forward for the incorporation of FFT with local texture descriptors so that the image forgery was detected with the help of traditional block-based method. The CASIAv1.0 data set was employed for testing the performance of utilized method and descriptors. Different standard detection parameters like precision and recall were considered to compute the outcomes.

H. Kasban, et.al (2020) stated that the major intend was to present an approach to detect the forgery in digital image [23]. This approach was capable of sensing any small image tampering and robust to

image manipulation attacks. Initially, the RGB image was transformed into YCbCr space in this approach. Subsequently, the extraction of Hilbert–Huang Transform (HHT) attributes was done from the Cr. The image was categorized as genuine or fake by testing and comparing three diverse classification algorithms namely SVM, KNN and ANN. The SSIM parameter was utilized to determine the outcomes so that the DR of forgery was computed. The outcomes depicted that Support Vector machine (SVM) provided a greater precision in contrast to other algorithms.

Youssef William, et.al (2019) suggested the forgery image detection methods for two common image tampering methods [24]. The match points methodology was implemented when the attributes were extracted through SIFT and SURF. The splicing was detected by extracting the edges of the integral images of Y, C b, and C r image components. Gray Level Co-occurrence Matrix (GLCM) was executed for every edge integral image and the feature vector was constructed. Afterward, the Support Vector machine (SVM) classification algorithm made the utilization of feature vector. The outcomes demonstrated that the efficiency of SURF over Scale-invariant feature transform (SIFT). The accuracy to detect the tempered images was obtained about 80%. Additionally, the finest outcomes were obtained while detecting the splicing image when the image was processed in YC b C r color model. The TPR was computed 99% in the detection of splicing images.

Navya Sara Monson, et.al (2017) introduced a FD approach in which fine inconsistencies were utilized in the color of the lighting of images [25]. This approach was based on ML that employed a behaviour knowledge space. The images which had two or more people were deployed in this approach. The forgery was detecting by combining the complementary illuminate estimators on image regions of similar material. These illuminate estimates assisted in extracting the attributes based in color, texture and edge. Later on, these attributes were used in ML to make the decision automatically.

Khizar Hayat, et.al (2017) recommended a technique to detect the forgery on the basis of DWT and DCT so that the attributes were mitigated [26]. The individual blocks were achieved when the discrete wavelet transform (DWT) image was split. These blocks were deployed in the discrete cosine transform (DCT). Afterward, the comparison of blocks was done on the basis of correlation coefficients. The recommended technique was tested by constructing a tampering method based on mask. This technique provided superior outcomes to other techniques.

GonapalliRamu, et.al (2017) intended a technique in which Scale-invariant feature transform (SIFT) algorithm was utilized. This technique had robustness and less complexity. The matched regions were extracted using the RANSAC algorithm [27]. The results of experiment demonstrated that the intended technique was capable of generating exact results in contrast to traditional technique utilized to detect the forgery. In addition, the features were matched and the tampered region was extracted applying Random Sample Consensus (RANSAC). The accuracy obtained on dataset that included eighty images was evaluated 98%.

Amira Baumy, et.al (2017) focused on implementing the high-pass filtering and histogram equalization as pre-processing phases for supporting the details of the images prior to detect the forgery [28]. A higher precision was obtained for classification using the detail reinforcement procedure. The Illumination histogram was estimated following the pre-processing. The peak value of the histogram derivative was considered as a parameter to detect the forgery. This paper also made the execution of thresholding approach. The classification was performed using the PDFs of the histogram derivative peaks.

Na Huang, et.al (2018) designed a CNN framework for understanding the derived attributes from each convolutional layer and detecting several kinds of image tampering by the means of automatic feature learning [29]. The CASIAv1.0 publicly available dataset having authentic images and splicing images was employed to conduct the experiments. The modification of this dataset included the retouching images and re-compressing images as the training data. The results proved that the designed framework was efficient and adaptable.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 8, Issue 7, July 2021

2.1. Comparison Table

Author	Year	Technique	Outcome
Tingge Zhul	2019	A forgery detection technique on the basis of LBP residue classes and color regions. The partition of an image was done into overlapped blocks. The evaluation of LBP residue classes was performed for every block. The plane generated through 'a' dimensional and 'b' dimensional from Lab color space was split into sixteen regions.	It provided the greater speed as compared to exhaustive search and comparative detection results simultaneously.
Navdeep Kanwal	2019	The methods of forgery detection executed into 2 domains of image forgery: CMFD and ISD. A detailed comparative analysis was carried out to make the utilization of local texture descriptors such as LBP and LTP in detecting the forgery of an image.	The CASIAv1.0 data set was employed for testing the performance of utilized method and descriptors. Different standard detection parameters like precision and recall were considered to compute the outcomes.
H. Kasban	2020	The major intend was to present an approach to detect the forgery in digital image. This approach was capable of sensing any small image tampering and robust to image manipulation attacks.	The outcomes depicted that Support Vector machine (SVM) provided a greater precision in contrast to other algorithms.
Youssef William	2019	The forgery image detection methods for two common image tampering methods. The match points methodology was implemented when the attributes were extracted through SIFT and SURF.	The accuracy to detect the tempered images was obtained about 80%. Additionally, the finest outcomes were obtained while detecting the splicing image when the image was processed in YC b C r color model.
Navya Sara Monson	2017	This approach was based on ML that employed a behavior knowledge space. The images which had two or more people were deployed in this approach.	These illuminate estimates assisted in extracting the attributes based in color, texture and edge. Later on, these attributes were used in ML to make the decision automatically.
Khizar Hayat	2017	A technique to detect the forgery on the basis of DWT and DCT so that the attributes were mitigated. The individual blocks were achieved when the discrete wavelet transform (DWT) image was split.	The recommended technique was tested by constructing a tampering method based on mask. This technique provided superior outcomes to other techniques.

Gonapalli Ramu	2017	A technique in which Scale-invariant feature transform (SIFT) algorithm was utilized. This technique had robustness and less complexity.	The accuracy obtained on dataset that included eighty images was evaluated 98%.
Amira Baumy	2017	The high-pass filtering and histogram equalization as pre-processing phases for supporting the details of the images prior to detect the forgery.	The classification was performed using the PDFs of the histogram derivative peaks.
Na Huang	2018	A CNN framework for understanding the derived attributes from each convolutional layer and detecting several kinds of image tampering by the means of automatic feature learning.	The results proved that the designed framework was efficient and adaptable.

CONCLUSION

In this work, it is concluded that there are several factors that must be considered while developing a copy-move forgery detection (CMFD) method. First of all, CMFD must be able to provide highly accurate and reliable detection results. However, the developed technique is also required to be effective in the context of speed and computational intricacy in real-time. The image blind detection has various phases which include pre-processing, feature extraction and classification. In future novel method will be proposed for the image blind detection.

REFERENCES

[1] X. Kang, and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics", 2008, in International Conference on Computer Science and Software Engineering, volume 3, issue 10, pp. 92630.

[2] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," 2008, in Pacific-Asia Workshop on Computational Intelligence and Industrial Application, volume 2, issue 15, pp. 2726.

[3] G. H. Li, Q. Wu, D. Tu, and S. J. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWTand SVD," 2007, in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing, volume 23, issue 15, pp. 17503.

[4] M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," 2011, in 18th IEEE International Conference on Systems, Signals and Image Processing (IWSSIP), volume 12, issue 4, pp. 14.

[5] I. Amerini et al., "A SIFT-based forensic method for copymove attack detection and transformation recovery", 2011, IEEE Trans. Inf. Foren. Sec., volume 6, issue 3, pp. 1099111

[6] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy move forgery in digital images," 2003, in Proceedings of the Digital Forensic Research Workshop, volume 17, issue 3, pp. 58.

[7] A. C. Popescu, and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," 2004, Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, volume 5, issue 2, pp.34-40

[8] Parul sharma, Harpreet Kaur, "Copy-Move Forgery Detection with GLCM and Euclidian Distance Technique in Image Processing", 2019, International Journal of Recent Technology and Engineering (IJRTE), volume-8, issue- 1C2, pp. 43-47

[9] M. AlSawadi, G. Muhammad, M. Hussain and G. Bebis, "Copy-Move Image Forgery Detection Using Local Binary Pattern and Neighborhood Clustering",2013, Modelling Symposium (EMS), volume 5. issue 13, pp. 249-254

[10] H. Yao, T. Qiao, Z. Tang, Y. Zhao and H. Mao, "Detecting CopyMove Forgery Using Non-Negative Matrix Factorization," 2011, Third International Conference on Multimedia Information Networking and Security, volume 8, issue 18, pp. 591-594.

[11] Yanjun Cao, T. Gao, and Qunting Yang, "A robust detection algorithm for copy-move forgery in digital images", 2012, Forensic Int., volume 214, issue 7, pp. 33-43
[12] Salam A.Thajeel, Ghazali Sulong, "A Survey of Copy-Move Forgery Detection Techniques", 2014, Journal of Theoretical and Applied Information Technology, volume 70 issue 1, pp. 25-35
[13] Saba Mushtaq and Ajaz Hussain Mir, "Image Copy Move Forgery Detection: A Review", 2018, International Journal of Future Generation Communication and Networking, volume 11, issue 2, pp.11-22
[14] Chengyou Wang, Zhi Zhang and Xiao Zhou, "An Image Copy-Move Forgery Detection Scheme Based on A-KAZE and SURF Features", 2018, Symmetry, volume10, issue 706, pp. 1-20
[15] Younis E. Abdalla1, M. Tariq Iqbal and M. Shehata, "Copy-Move Forgery Detection Based on Enhanced Patch Match", 2017, International Journal of Computer Science, volume 14, issue 6, pp. 1-7
[16]K Sudhakar, V. M. Sandeep, Subhash Kulkarni, "Speeding-up SIFT based copy move forgery detection using level set approach", 2014, International Conference on Advances in Electronics Computers and Communications
[17] Ghulam Muhammad, Muhammad Hussain, Anwar M. Mirza, George Bebis, "Dyadic wavelets and DCT based blind copy-move image forgery detection", IET Conference on Image Processing (IPR 2012)
[18] Güzin Ulutaş, Mustafa Ulutaş, Vasif V. Nabiyev, "Copy move forgery detection based on LBP", 2013, 21st Signal Processing and Communications Applications Conference (SIU)
[19]Hieu Cuong Nguyen, Stefan Katzenbeisser, "Detection of Copy-move Forgery in Digital Images Using Radon Transformation and Phase Correlation", 2012, Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing
[20] S. A. Fattah, M. M. I. Ullah, M. Ahmed, I. Ahmmed, C. Shahnaz, "A scheme for copy-move forgery detection in digital images based on 2D-DWT", 2014, IEEE 57th International Midwest Symposium on Circuits and Systems (MWSCAS)
[21] TinggeZhul, Jiangbin Zheng, Yi Lai, Ying Liu, "Image blind detection based on LBP reside classes and color regions", 2019, PLoS ONE
[22] Navdeep Kanwal, Akshay Girdhar, Lakhwinder Kaur, Jaskaran Singh Bhullar, "Detection of Digital Image Forgery using Fast Fourier Transform and Local Features", 2019, International Conference on Automation, Computational and Technology Management (ICACTM)
[23] H. Kasban, Sabry Nassar, "An efficient approach for forgery detection in digital images using Hilbert–Huang transform", 2020, Applied Soft Computing
[24] Youssef William, SherineSafwat, Mohammed A.-M. Salem, "Robust Image Forgery Detection Using Point Feature Analysis", 2019, Federated Conference on Computer Science and Information Systems (FedCSIS)
[25] Navya Sara Monson, K.V. Manoj Kumar, "Behavior knowledge space-based fusion for image forgery detection", 2017, International Conference on Inventive Communication and Computational Technologies (ICICCT)
[26] Khizar Hayat, Tanzeela Qazi, "Forgery detection in digital images via discrete wavelet and discrete cosine transforms", 2017, Computers & Electrical Engineering
[27] GonapalliRamu, S. B. G. Thilak Babu, "Image forgery detection for high resolution images using SIFT and RANSAC algorithm", 2017, 2nd International Conference on Communication and Electronics Systems (ICCES)
[28] Amira Baumy, Mahmoud Abdalla, Naglaa F Soiliman, Fathi E. Abd El-Samie, "Efficient implementation of pre-processing techniques for image forgery detection", 2017, Japan-Africa Conference on Electronics, Communications and Computers (JAC-ECC)
[29] Na Huang, Jingsha He, Nafei Zhu, "A Novel Method for Detecting Image Forgery Based on Convolutional Neural Network", 2018, 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)