ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 7, Issue 11, November 2020

A Review on Various Copy Move Forgery Detection Techniques and Popularly used Benchmark Datasets

[1] Alok Kumar Singh
[1] ME CSE Student NITTTR Chandigarh Panjab University
alok.singh97@gmail.com.

Abstract: Image processing is one of the most demanding research areas now a day because various fields like medical, engineering, research, industry, e-commerce business etc. mainly based on digital images. It attracts researcher's focus because any tampering on authenticated digital images may changes the whole result. It faces misuse of original documents by unauthorized users. From the beginning of research in image processing field researchers tried to develop effective algorithms that prevent the digital images from any tampering attacks. There are many types of tampering like copy-move, image splicing and image resampling perform on digital images. The tampering operation (TO) on digital images mainly divided into two types: The first one is Active Tampering operation and second one is Passive tampering operation. In this paper we try to focus on various copy-move forgery detection (CMFD) methods that come in passive image tampering like PCA, SIFT, SURF etc. It may be block based and key point-based methods. The acceptance of developed algorithm increased widely if it performs effectively on benchmark datasets. We also cover some of demanding datasets for copy-move tampering operation like MICC F-220, CoMoFoD etc.

Keywords— Copy Move Forgery Detection (CMFD), Tampering Operation (TO), PCA, SIFT, MICC F-220.

I. INTRODUCTION

Image tampering or forgery is the way through which anyone can create duplicate or altered image. The aim of doing tampering is to get benefits like an authorized user. There are many commercial and open source image editing software's are easily available that are used to manipulate the digital images. By using these software's anyone can easily change the content without effecting their quality.

Image tampering is primary issue that challenges the security of digital images. Most of the area of today's world depends on digital images for any evidence and communication.

Now's a day electronic device is not costly compare to initial days. Anyone can easily purchase the good quality digital cameras and easy availability of image editing software's anyone can manipulate the digital image. It doesn't matter the attacker is professional or not.

Image tampering detection method categorized into two main parts: active and passive method. In this paper our focus is to cover passive image tampering detection methods.

Passive digital image tampering divided into two area i.e. first one is tampering and second one is source device. Our focus is on tampering area. It breaks into two parts i.e. dependent and other is independent. Copy-move comes in dependent area.

Following are the different image tampering method to perform changes in digital images:

Copy-move forgery: In copy-move some of the area of a single image is copied and pasted on other area of the same image. Identify the changes is not an easy task for users. Level of similarity of forgery area is almost same as the actual image. So, security concern of digital images is becoming very complex.

Image Splicing: In image splicing more than one images are merged. for tampering detection point of view this one complex compare to copy-move because in a single images various textures are available and features also.

Image Retouching: In image retouching main focus is to create high level of similarity in appearance of a digital image. It looks similar to actual image. Try to create effective background by using more than one color.

If effective detection algorithms are essential for tampering detection in digital images. The benchmark dataset is also a core part of forgery detection because without effective dataset we cannot check the strength of our developed detection method. In this paper we cover some common benchmark datasets like MICC F-220, CASIA etc.

II. RELATED WORK

In the field of digital image processing, image tampering is the demanding research area. The main focus on passive image tampering detection. The passive image tampering detection is categorized into two types: first

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 7, Issue 11, November 2020

one is block -based detection method and second one is key point-based detection method.
Some effective work done in past related to passive forgery.

Popescu et.al [7] used PCA to find out the features from the digital image and also reduce the features dimension.

Christlein et.al.[8] covered many feature extraction methods for forgery detection in digital images.

Amerini et.al.[6] covered SIFT method for key point based digital image forgery detection.
Some of the authors used benchmark datasets for effective detection results:
Mohammad Farukh Hashmi et.al [4] uses MICC F- 220 benchmark datasets for effective output.

Reshma Raj and Niya Joseph [5] find out the effective result on their proposed method on using benchmark dataset MICC F-600.
Hesham A. Alberry et.al [2] used MICC F-220 datasets on their proposed method and find out the better result.

In past years many researchers tried to develop more effective detection algorithms to rectify the digital image tampering operation.

To study various authors, work on tampering detection algorithm that helps to sort out the gap between previous work and recent development in detection strategies.

III. WORKFLOW FOR COPY-MOVE FORGERY DETECTION

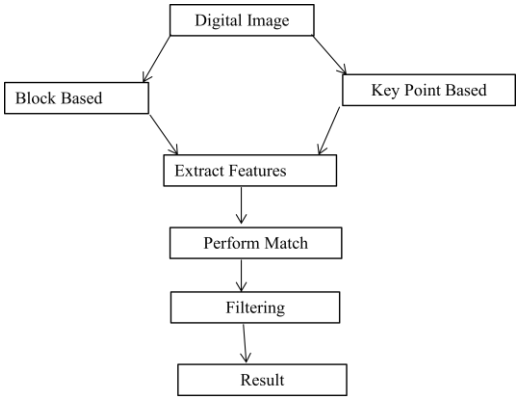


Fig: 1 Fundamental Workflow of Copy Move Forgery Detection

Every researcher follows the same workflow for copy-move forgery detection. In first step pre-processing operation is performed. In pre-processing step all the data related to a digital image is prepared for processing by using feature of an image.

After this step feature extraction is done, all the tampering detection based on features. Then matching operation is performing to find out the dissimilar region to detect image tampering.
Before find out the result filtering process is done to effectively find out the area where tampering is performed.

IV. BLOCK BASED COPY-MOVE FORGERY DETECTION METHODS

Following are the various block-based Copy -move forgery detection methods:

A. PRINCIPLE COMPONENT ANALYSIS (PCA) METHOD:

PCA method comes under the category of block-based method; input image is divided into many blocks.
In PCA, statistical analysis is done and find out the correlation between various components. The primary concern of PCA method is to find out the pattern in available data.

For any parameter we find out the many features, but all the features are not useful, we have to reduce the dimension.
To find out the tampered area in an image not an easy task and if tampering is done on more than one area it becomes more tedious job. PCA method is effective in such type of conditions and gives effective results.

B. DISCRETE WAVELET TRANSFORM (DWT) METHOD:

In DWT, the wavelet is nothing but it is mathematical function.
Following are the essential point that attracts researchers to focus on DWT in forgery detection:

- When signal discontinuities arise, Wavelet Transform generates less coefficients compare to Fourier transform.
- Wavelet transform represents signals in better way compare to other transformation methods.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 7, Issue 11, November 2020

- First wavelet breaks available data into various frequency components after that analyse each components resolution.
- The main purpose of using DWT is to observe discontinuities of the signal.
- Useful in many application area's like digital image compression and earthquake prediction.

C. DISCRETE COSINE TRANSFORM (DCT) METHOD

- In DCT core work is transformation of a digital image. Like an image in spatial domain is converted in Fourier Transform using DCT.
- The main benefits of using DCT are JPEG Compression of image that helps at transmission time. The length of an image and other complex issues that creates problems at the time of transmission is solved by using compression techniques.
- To perform compression, we need two essential steps i.e. Quantization and Entropy Coding.

D. FOURIER TRANSFORM METHOD

Fourier transform is a widely used transformation method.

Following are the various point that represent the significance of Fourier transform:

- In digital image processing it help to extract the feature of a block.
- It is used to find out the frequency of a digital image.
- More than one frequency coefficients are generated but for single block we have to find out the best one that is used as block representative.

V. KEY POINT BASED COPY MOVE FORGERY DETECTION

Following the most popular key point based copy move forgery methods:

A. SCALE INVARIANT FEARURE TRANSFORM (SIFT)

SIFT is a popular key-point based approach. In Key point-based approach we have to focus on two essential points i.e. interest point detector and robust local descriptors.

One thing that attracts our interest is how we can extract key point by using SIFT approach. Following are the essential point that used in key-point extraction:

- Scale space peak
- Localization of key points
- Assignment of orientation
- Key point descriptors

B. SPEED UP ROBUST FEATURES (SURF)

SURF performs better in some parameters over SIFT and gain popularity.

- The first one is feature vector dimension; SURF uses 64-dimensional feature vector but SIFT uses 128-dimensional feature vector because of this SURF is fast compare to SIFT
- The second one is matching process, SURF uses hessian matrix for matching trace, it's better than SIFT.

VI COPY-MOVE FORGERY DETECTION POPULAR DATASETS

A. MICC DATASETS

To find out the effective result we need both i.e. powerful detection algorithm and effective datasets that check the strength of detection algorithm.

- We have some well-known datasets that frequently used by researchers. MICC dataset is one of them. MICC datasets have subgroups like MICC F-220, MICC F-600 and MICC F-2000.


Following table show descriptions of MICC datasets with some essential parameters:

ISSN (Online) 2394-6849

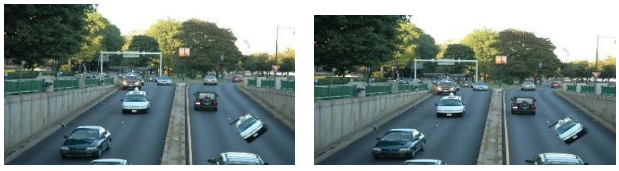
International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 7, Issue 11, November 2020

Table.1 List of various MICC's datasets

Subgroup	Total	Tampered	Non Tampered	Image size
MICC F-220	220	110	110	722x480 to 880x600
MICC F-600	600	160	440	800x533 to 3888x2592
MICC F-2000	2000	700	1300	2048x1536

Table2. Effective results obtained by authors using MICC-F220 dataset.

Author	Result
Hesham A. Alberry et.al 2018[2]	Average detection time reduced by 15.91%
Diaa M Uliyan, Hamid A. Jaleb et.al 2016	TPR=96.5 and FPR=2.86
Kakar and Sudha 2012	TPR=90 and FPR=3
Mishra et.al 2013	TPR=73.6 and FPR=3.64



(a) Actual Image (b) Tampered Image

Fig: MICC-F220 Datasets

B. CoMoFoD DATASETS

- CoMoFoD dataset is also a frequently used datasets for image tampering detection. It consists of 260 images. The size of each image is of two types one 512x512 small type and another one is 3000x2000 large types.

(a) Actual Image (b) Tampered Image

There are five types of manipulations available in CoMoFoD dataset. The manipulations such as:

- Scaling
- Rotation
- Distortion
- Combination
- Translation

Table.3 Effective results obtained by authors using CoMoFoD datasets.

Author	Result
Chen Ming Hsu et.al.[10]	CDR(correct Detection Ratio) is higher than 0.9
Meera Mary Issac et.al [15]	Precision=0.99

VII CONCLUSION

When we observe today's requirement in terms of digital image, most of the area need digital images for communication, evidence, business, medical, education etc. One crucial issue arises in all area that is authenticity of digital images.

To protect digital images from attackers, we have to develop secure detection algorithm. Lot of effective detection algorithm available in image forensic field that identify the forged digital images but attackers also tries to develop new strategies to do tampering in digital images. Along with powerful tampering detection algorithms we need strong benchmark datasets that check the effectiveness of developed detection algorithm.

In future the field of digital image forensic requires various new detection algorithms and new datasets to detect the tampering operation on digital images.

REFERENCES

[1] Nor Bakiah Abd Warif, et al, "Copy-move forgery detection: Survey, Challenges and future directions", Journal of Network and computer applications 755(2016)259-278.

[2] Hesham A. Alberry, Abdelfattah A. Hegazy et.al, "A fast SIFT based method for copy move forgery detection", Future Computing and Informatics Journal 3(2018)159-165.

[3] Devanshi Chauhan, Dipali Kasat, Sanjeev Jain, "Survey on Key point-based Copy-move Forgery

Detection Methods on Image, Procedia Computer Science 85,206-212,2016.
[4] Mohammad Farukh Hashmi et.al"Copy Move Forgery Detection using an Efficient and Robust Method Combining undecimated Wavelet transform and Scale invariant Feature Transform", AASRI Procedia 9(2014)84-91.
[5] Reshma Raj, Niya Joseph, "Key point Extraction Using SURF Algorithm for CMFD", Procedia Computer Science 93,375-381,2016.
[6] I.Amerini,L.Ballan et.al, , "A SIFT based Forensic method for copy-move attack detection and transformation recovery" IEEE Transactions on Information Forensics and Security,vol.6,iss.3pp.1099-1110,2011
[7] A.Popescu and H.Farid, "Exposing digital forgeries by detecting duplicated image regions," Department of Computer Science,Dartmouth College,Tech .Rep.TR2004- 515,2004.
[8] Vincent Christlein et.al, , "An Evaluation of Popular Copy-Move Forgery Detection Approaches" in IEEE Transactions on Information Forensics And Security,pp.1841- 1854,2012.
[9] Anil Dada Warbhe, R.V. Dharaskar, V.M. Thakare, "A Scaling Robust Copy-Paste Tampering Detection for Digital Image forensics", Procedia Computer Science 2016.
[10] Chen-Ming Hsu, Jen Chun Lee, "An Efficient Detection Algorithm for Copy-Move Forgery", IEEE978-1-4799-1989 (2015).
[11] Meera Mary Isaac , "Image Forgery Detection Based on Gabor Wavelets and Local Phase Quantization", Procedia computer Science 58,76-83,2015.
[12] Jian Li, Xiaolong Li, Bin Yang, "Segmentation Based Image Copy-Move Forgery Detection Scheme, IEEE Transactions on Information Forensics and Security", Vol.10, No.3, March 2015.
[13] H.Huang,W Guo and Y.Zhang, "Detection of Copy-move forgery in digital images using SIFT algorithms,in proc.Pacific-Asia Workshop Comut.Intell. Ind Appl.(PACIIA),Dec 2008,pp.272276
[14] S.Bayram ,H Sencar and N.Menon,, "An efficient and robust method for detecting copy-move forgery,"in IEEE International Conference on Acoustics,Speech and Signal Processing,Apr.2009,pp.1053-1056.
[15] J.Fidrich,D.Soukal et.al., "Detection of copy-move forgery in digital images," in Proceeding of Digital Forensic Research WorkshopnAug.2003.