A Review of Literature On copy-move forgery detection techniques

Sawinder Singh Mangat[1]Harpreet Kaur[2]
[1]P.G Student [2]Assistant Professor
[1]Department of Electronics and Communication
[2]Department of Computer and Science
[1,2]Chandigarh University, Gharuan, Mohali
[1]shavisinghmangat@gmail.com
[2]harpreet8307@gmail.com

***Abstract*: Copy-move is one of the important image forgery parts. Copy-move image forgery detection need big attention as compare to all other forgery methods because copy-move image forgery detection is used in forensic laboratories. In this paper, all algorithm used in copy-move forgery detection are reviewed. All algorithm comparison is also done in paper with some comparison tables and some graphs. We also discuss keypoint based methods and block based methods and some future research directions were also pointed out.**

Keywords: **Digital image, Forgery detection, copy-move forgery,Image retouching**

I. INTRODUCTION

In this modern era, "we are seeing a figure is not conceivable because there are lots for changes has been done to hide or to add some information or some objects". Automation today makes it easy for anyone with a computer to modify official documents, including photos, changing material content. Receiver of this material might process these digital forgeries unless they have controls in place to verify key information. Nowadays digital image can be easily manipulated by some powerful tools, such as adobe Photoshop, etc. some tools are free whereas some are licensed. These tools make it very easy to create a forged image from one or more than one image. Image forgery detection has being emerged as a remarkable research in applications of computer vision, digital image processing, biomedical technology, criminal investigation, image forensics, etc. It becomes more attractive and challenging when powerful software tools for image processing are so popular and sophisticated that we cannot confirm whether image is manipulated by naked eyes.[1] As example of newspaper (e.g. refer figure-1), in which three photographs were used to create a one forged image. Image of white house, Bill Clinton, Saddam Hussain. Firstly Image of white house is blurred to create an illusion of an out-of-focus background. Then, image of Bill Clinton and Saddam Hussain were cut from two different images and pasted in white house image.

Detecting that hidden object or information is very challenging task because we can't recognize the forged image by naked eyes. There are some techniques to detect that forged part which depend on the techniques which are used to create forged image.


INTERNET

Spies turn to high-tech info ops

PCs, Internet used for manipulating images, public opinion

ALTERED IMAGE

BY DANIEL VERTON

Federal intelligence agencies are studying ways to use computers and the Internet, rather than just leaflets and radio broadcasts, to shape and disseminate information designed to sway public opinion in the world's hot spots.

As part of its so-called "perception management" program, the intelligence community has for decades created misinformation to trigger political change without direct political or military involvement in countries where the United States has vested interests, such as Iraq and North Korea.

Acting on congressional recommendations to bolster research and development in information technology, intelligence agencies are turning to PCs to develop more sophisticated means of manipulating and delivering digital photos, video clips and recorded sound to portray fictitious events in hopes of provoking desirable outcomes.

1 2 3

Altered Egos

The top photo, of a fictitious meeting between President Clinton and Saddam Hussein, was generated by digitally altering and combining elements from three photos, shown below the altered image. Intelligence agencies plan to use similar techniques to create images and then disseminate them via the Internet in their efforts to influence events in foreign countries, such as Iraq.

Fig-1: example of copy-move forgery

II. TYPES OF IMAGE FORGERY

Creation of forged image is classified into three parts as follows:

1. Copy-move forgery
2. Image forgery using splicing
3. Image retouching

Explanation of all different parts:

1. *copy-move forgery:-*

This is most commonly used image tempering method. In this a part of the source image is first taken out and then copied to other parts once or may be multiple times to hide or add some information. Copy-move is also known as cloning. Copied part is taken from same image. In simple word, we can say that source image and destination image is same**.** In Copy-move forgery, Copied regions in image can be post processed, rotated flipped and scaled before pasting to other places to hide or remove any details. Example of copy-move image forgery is presented in fig-2**.** [2]

Fig-2: example of copy-move forgery; (left) original image with three missiles; (right) forged image with four missiles [2]

Copy-move forgery is divided into mainly two groups namely: **keypoint based methods** and **block based method**. We can say that Keypoint based methods are same as suspicious points. They are spatial locations or points in the image that define what is interesting or what is stand out in the image.

Keypoint is better than block based method because no matter if there is rotation in image or distorted, keypoint always define interesting points. Whereas in block based method, image is separated into small overlapping or non-overlapping blocks. For analyzing the matching area of image, these blocks are compared with each other.

2. image forgery using splicing:

In this technique, there are more than one source images from where some part of image is taken to create a new fake (forged) image.

Fig-3: example of image forgery using splicing

As in fig-3: first image of helicopter is turned over horizontally and then add another image of 'The shark' to create a new fake image. Image splicing involves composite of two or more than two images which are combined to create a forged image.

3. image retouching:

Image retouching is less harmful than other forged images. In this, image is not significantly change, but instead, enhances or reduces certain features of an image as shown in fig-4. In this method, the professional image editors adjust colors, change background and work with hue saturation for toning and balancing. Image retouching is mostly used for fashion, beauty or advertising photos, interesting images for advertisement.

Fig-4: example of image retouching

III. LITERARUTRE SURVEY ON COPY-MOVE IMAGE FORGERY DETECTION TECHNIQUES

In first survey [3],B.L. Shiva Kumar, Lt. Dr. S. Santhosh Baboodiscuss various methods of detecting copy-move image forgery in digital images. They compare region duplication detection with scaling and rotation and without scaling and rotation. They also discuss various challenges like tempered region with compression, tampered image with noise, tempered region with rotation.

In [4],Davide Cozzolino, Giovanni Poggi and Luisa Verdoliva propose an algorithm for accurate detection and localization of copy-move forgeries, based on rotation-invariance features computed densely on the image. In this algorithm, of dense field techniques, price of much higher processing time this is slow because of feature matching phase. This problem increases with increase in image size. And this problem is resolved by fast approximate nearest neighbor search algorithm to deal accurately with invariant feature, to achieve high robustness with rotation and scale images. And also reduce the overall complexity by implementing a fast-post-processing procedure which is based on dense linear fitting.

In [5],P. M. Panchal, S. R. Panchal, S. K. Shah present the comparison of two keypoint algorithm SIFT (Scale Invariant Feature Transform) & SURF (Speed Up Robust Feature). Both are used to point-out the distinctive invariant features from an image that can be used to compare different angles of image. Comparisons of both SIFT & SURF is shown in table-1.

Based on comparison it is shown that SIFT detect more feature points as compare to SURF and matched feature point in SIFT is more than SURF but SIFT consume more time for feature detection as compare to SURF.

SIFT is used for extracting features from an image that can invariant to image scale and rotation whereas SURF use integral images for image convolution and fast-hessian detector.

Algorithm	Detected feature Points		Matching feature point	Feature matching Time
	Image1	Image2		
SIFT (Scale Invariant Feature Transform)	892	934	41	1.543 s
SURF (Speed Up Robust Feature)	281	245	28	0.546 s

Table-1: Comparison of results of both SIFT& SURF

Parameters	T_p	T_N	F_P	F_N	Precision (p)	Recall (r)	False Positive Rate (FPR)
SIFT	82	106	4	28	95%	74%	4%
DyWT +SIFT	88	99	11	22	88%	80%	10%

Table-2: comparison of performance

SIFT algorithm has four steps:-

a. Scale space extrema detection:-
In first step location is identified and keypoints using scale space extrema in DOG (Difference-of-Gaussian) function.

b. Keypoint localization:-
In this step, keypoint candidates are localized & eliminate the low contrast keypoints.

c. Orientation assignment:-
In this, keypoint is obtained based on local image gradient.

d. Description generation:-
In this step, compute each keypoint based on image gradient magnitude & orientation at each sample point at region centered keypoint.

Whereas, in **SURF** algorithm, feature detection is based on hessian matrix because hessian matrix has better performance and accuracy is also better.

In [6], Mohammad Farukh Hashmi, Vijay Anand, Avinas G. Keskar introduce a hybrid method for copy-move forgery detection by combining Dyadic Wavelet Transform(DyWT) & Scale Invarient Feature Transform (SIFT). In this hybrid technique, DyWT is applied firstly ona given image to decompose it into four parts LL,LH,HL and HH.as in given image LL part contains most of the information then secondly, they apply SIFT on LL part only to extract key feature and find description vectir of these keypoints and then find similar descriptor vector to conclude about copy-move forgery is done in given image. Author also tell us why they use DyWT instead of DWT bacause DWT has limitaion that it is shift invarient and less optimal for data analysis. So, author use DyWT to ovecome limitaions of DWT because in DyWT, there is no down sampling is done in DyWT like in that of DWT. Comparison of proposed algorithm performance with SIFT is shown in given table-2.
Where,
T_p = number of imagesthat have been correctly detected as forged
F_p= number of images that have been falsely detected as forged
F_n= number of images that have been falsely missed but they are forged

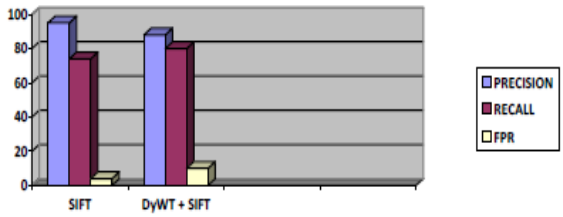

Fig-5: performance parameters of proposed method

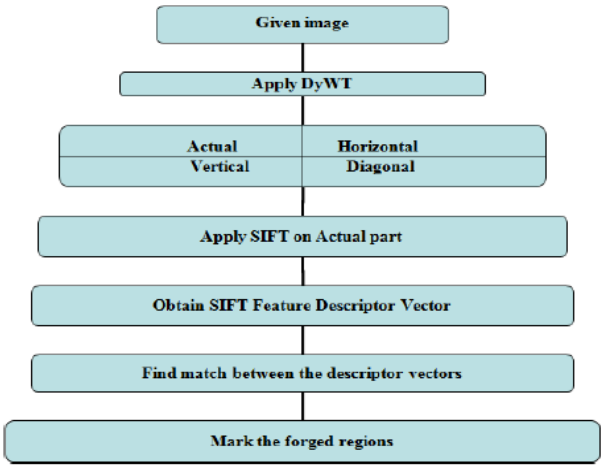

Fig-6: block diagram of proposed algorithm

In **[7],**Weihai Li and Nenghai Yu introduce a rotation robust detection of copy-move forgery. They propose a algorithm depend upon Fourier-Mellin Transform(FMT) with feature extracted along radius direction. They use link processing instead of hash value counting in the counting bloom filters to reduce the computational cost. This improved algirithm is good to duplicate region of large rotation angle. FMT also robust to lossy compression,scaling and rotating operations. In conclusion, author also suggest future work to face the problem of noise robust, high scaled copy-paste area.

In [8],Prema.C, Percy Granaph.J, Angaline.S, Thanga Belsi.I proposed algorithm by using k-d tree (K-dimensional tree) algorithm for matching pattern because k-d tree is much faster than other algorithms. Author use various transformation from which the forged region can be identified by estimating transform between matched SIFT keypoint. Author use SIFT algorithm with k-d tree and RANSAC (Random Sample Consensus) algorithm regions very accurately.

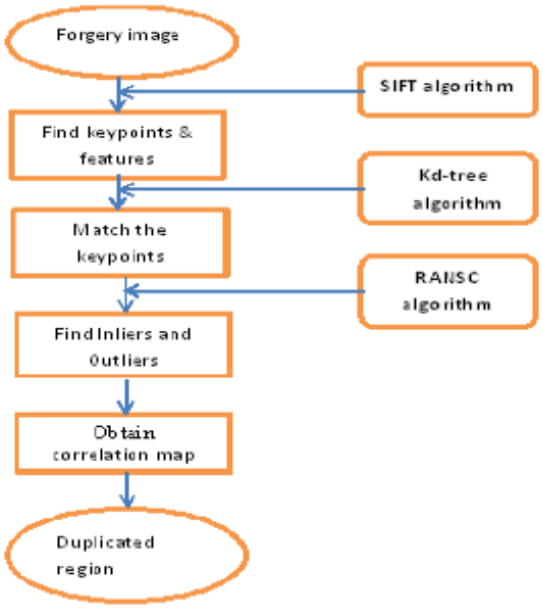

Fig-7: flow chart of proposed algorithm

in research, author first find image keypoints using SIFT algorithm then that keypoints are matched by using k-d tree algorithm but that matched keypoints are inacurate due to large number of mismatch keypoints. Author use RANSAC to find out the unreliable keypoints then author identify duplicated regions. This hybrid technique is usefull in presence of additive noise and for different JPEG qualities.

In [9], Chen-Ming Hsu, Jen-Chin Lee, Wei-Kuei Chen compare all different methods used to detect copy-move forgery and propose algorithm based on Histogram of oriented Gabor magnitude (HOGM) of overlapping blocks. Author introduce following steps for detection of copy-move forgery:-

I. Feature extraction with Gabor Magnitude
II. Dividing image into overlapping blocks
III. Obtaining HOGM descriptors of same size
IV. Comparison of HOGM features in each block
V. Post-Processing of detection result

Block size	16 × 16	32 × 32	48 × 48
CDR	0.997	0.986	0.912
FDR	0.003	0.013	0.124

Table-3: comofd results of proposed algorithm

In table-3, author give results of different size of blocks (16×16, 32×32, 48×48) we can see that. Correct detection ratio (CDR) is better than false detection ratio (FDR).

Methods	Number of Block	Feature Dimension
PCA	255,025	64
Proposed	247,009	12

Table-4:comparison of two forgery detection approaches

in another survey [10], Harpreet Kaur, Jyoti saxena and sukhjinder singh compare all the keypoint based copu-move forgery detection and their hybrid methods. Keypoint methods like SIFT, SURF, ORB. Author explain allliterature survey about these algorithms with full explanation. According to them keypoint based methods are better than block based methods in terms of computational efficiency space complexity and robustness against rotation and scaling. They conclude that SIFT is better than ORB and SURF in terms of accuracy whereas in terms of time for detection ORB is faster than SURF and SIFT.

Preeti Yadav[11] introduce an improved algorithm by applying DWT into an image to reduce the dimension representation. The feature vectors will be extracted from the small overlapping blocks of the compressed image and sorted lexicographically to find the duplicate blocks. The detection was carried out on the lowest level image representation and also proved best performance on small copy-move forgery, detected the multiple copy-move forgery with lower computational complexity.

IV. CONCLUSION

In this paper, all methods of copy move forgery detection are reviewed. In conclusion, SIFT perform better than other algorithms in terms of feature detection but it consumes more time. SURF is used where time is less because SURF is speed-up version of SIFT but it is not better in feature detection. Our Future work is how we merge two algorithm for getting better results.

REFERENCES

[1] Luo Weiqi, Jiwu Huang and Guoping Qiu, "*Robust detection of region-duplication forgery in digital image*", 18th International conference on image recognition IEEE, Vol. 4, 2006.
[2] M. Ali Qureshi, M. Deriche, "*A review on copy-move image forgery detection techniques*".
[3] B.I. Shivakumar, Lt. Dr. S.Santhosh Baboo. "*detecting copy-move forgery in digital images: A survey and analysis of current methods*", Global journal of Computer science and technology, vol. 10, pp. 61-65, 2010.
[4] Davide Cozzolino, Giovanni Poggi and Luisa Verdoliva, "*Efficient Dense-field copy-move forgery detection*", IEEE Transaction on information forensics and security, vol. 10, No. 11, november 2015.
[5] P.M. Panchal, S.R. Panchal and S.K, Shah, "*A comparison of SIFT and SURF", International journal of Innovative Research in computer and communication engineering*" Vol. 1, april 2013.
[6] Mohammad Farukh Hashmi, Vijay Anand, Avinas G, Keskar, "*copy-move image forgery detection using efficient and robust method combining Un-decimated Wavelet Transform and Scale invarient Feature Transform*", AASRI conference on circuit and signal processing", Procedia 9, pp. 84-91, 2014.

[7] Weihai Li and Nenghai Yu, "*Rotation robust detection of copy-move forgery*", IEEE 17th International conference on image processing, sept, 2010.
[8] Prerna.C, percy Granaph.J, Angaline.S, Thanga Belsi.I, "*A keypoint based copy-move forgery detection*", international journal of advanced information science and technology, vol. 12, No. 12, April 2013.
[9] Chen-Ming Hsiu, Jen-Chun Lee and Wei-Kuei Chin, "*An efficient detection algorithm for copy-move forgery*", 10th Asia joint conference on Information security, 2015.
[10] Harpreet Kaur, Jyoti Saxena and Sukhjinder singh, "*Key-point based copy-move forgery detection and their Hybrid methods*", Journal of the International Association of Advanced Technology and science, Vol. 16, June 2015.
[11] Preeti Yadev, Yogesh Rathore, "*Detection of copy-move forgery of Images using Discrete Wavelet transform*", International Journal on computer science and Engineering(IJCSE), Vol. 4 No. 04, April 2012.