International Journal of Engineering Sciences & Research Technology

(A Peer Reviewed Online Journal)
Impact Factor: 5.164

IJESRT

RESEARCHERID
THOMSON REUTERS

[Kaur, *et al.*, 9(3): March, 2020]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

COPY MOVE FORGERY DETECTION IN DIGITAL IMAGES USING IMPROVED SIFT (I-SIFT) APPROACH

Lovepreet Kaur[*1] Sandeep Singh Dhaliwal[2]

[*1]M.Tech Student, BMS College of Engg., ShriMuktsar Sahib

[2]Assistant Professor, BMS College of Engg.,Shri Muktsar Sahib

DOI: 10.5281/zenodo.3700407

ABSTRACT

With this across the board use of computerized pictures, notwithstanding the expanding number of instruments and programming of advanced pictures altering, it has ended up being definitely not hard to control and change the genuine information of the image. Existing system for forgery detection has many problems like maximum angle that existing system can detect is 40 degree rotation. Existing systems cannot detect forgery if duplicate content is compressed or enhanced. In the proposed system, we have developed a novel approach namedI-SIFT for copy move forgery detection that can detect the copy move forgery in digital images. Proposed system is efficient in detecting the copy move forgery if forged area is compressed, enhanced or rotated up to 270 degree.

KEYWORDS: Copy- Move forgery Detection, Image forgery, M-SIFT Algorithm, Image Authenticity.

1. INTRODUCTION

Since images are instantaneous and their content can be easily understood - a privilege that is not found in texts - they are considered effective for human communication. Our visual system can derive pictorial information extremely faster than any other kind of information. Such information forms nearly 75% of information perceived by the visual system. The use of such pictorial information has increased and has become easier due to advances in digital photography. Nowadays a variety of applications rely on digital images. These include newspapers, tabloid magazines, scientific Journals, fashion industries, court halls and many others.

Today, almost everybody can record, store and share a large amount of digital images because of the spread of easy and cost effective device that enables the acquisition of visual data. At the same time, image editing software is widely available which makes it extremely simple to manipulate the content of the image. This can be achieved through creating new images by tampering and counterfeiting the visual content in an expert – like method. Current software allows users to create computer graphics that can't be distinguished from real photos or even to generate hybrid generated visual content.

Digital Image Forensic

Digital forensic science is a modern branch of science which aims to reconstruct events and identify entities involved. This field deals with the study of deciding the originality and reliability of digital media such as images. Strictly speaking, the term forensic implies the application of scientific approach on the investigation and detection of a crime. Such forensic analysis serves in providing proof or evidence at courts. Recently, Digital images have widely spread leading to the use of digital image forensic in broader context of situation.

Digital image forensic is a new discipline exploits image processing and analysis tools to recover information about the history of an image. The trustworthiness of any digital image must be ensured whenever such image is used to convey any piece of information. The trustworthiness of any image may verify the authenticity of the image which means that such image was not manipulated or counterfeited indicating a valid representation of the real world.

Three fundamental groups underlie the techniques of forensic digital images. These categories are: Detection of Computer Generated Images, Image Source Identification and Image Forgery Detection.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

2. LITERATURE SURVEY

S. Thakur et al.(2016), In this paper author describes that The image forensics is the technique which is applied to hide image important information. In the base paper, the technique of SIFT algorithm is applied to mark the objects in the image. In the SIFT algorithm whole image is scanned and from the scanned image objects are marked. The properties of the marked object are accessed and objects which have similar properties are classified into group and other are into second. To classify the similar type of objects techniques like block based & Key Point based technique, shift key point can be used[1].

Weihai Li et al. (2016) JPEG is probably the most widely used image compression standard in taking digital pictures, e.g., in most digital cameras. Thus, manufactured pictures by the trap operation of duplicate glue are as a rule from and to JPEG pictures. Understanding that it may be difficult to discover a strategy that is all inclusive for a wide range of falsifications, we proposed a novel visually impaired way to deal with identify duplicate glue trail in doctored JPEG pictures and in the mean time find the doctored region. The methodology functions admirably notwithstanding when a JPEG picture is truncated or multi-compacted, by concentrate the DCT piece ancient rarity network and identify confuse of the framework. Tests well exhibit the adequacy of the proposed approach[2].

C. Bhalla et al.(2016), Images now-a-days are often used as an authenticated proof for any crime and if these images does not remain genuine, it will create a problem. This leads to the problem of Image Forgery. Image Forgery is defined as adding or removing important features from an image without leaving any obvious traces of tampering. Further, it can either be intrusive (active) or non-intrusive (blind or passive). In active approach, the digital image requires some kind of pre-processing such as watermark embedded or signatures are generated at the time of creating the image. Passive image forensics is usually a great challenge in image processing techniques. It includes the concept of Copy-Move Forgery, Retouching and Image Splicing. In this paper, more of the research work is done on Image Splicing Techniques and Copy-Move Forgery. It includes the basic survey of various forgery detection techniques and the ways to cure the problem[3].

Joshi Chintal J et al. (2016),This paper reveals basics of Digital (Image) Forensics.One of the most successful application digital image forgery detection has recently received significant attention, especially during the past few years. No less than two pattern represent this: the main tolerating computerized picture as official record has turned into a typical practice, and the second the accessibility of ease innovation in which the picture could be effectively controlled. Despite the fact that there are numerous frameworks to recognize the computerized picture imitation, their prosperity is constrained by the conditions forced by numerous applications. Most existing strategies to distinguish such altering are fundamentally at the expense of higher computational many-sided quality. Duplicate Move fabrication is a particular kind of picture imitation, in which a piece of computerized picture is replicated and glued to another part in the same picture. In this paper we propose a strategy to distinguish copied districts in a picture utilizing Zernike minutes. By utilizing Zernike minutes we can distinguish copied locales regardless of the possibility that they scaled or turned, however these elements can't discover level copied areas. Zernike minutes can take care of this issue; we will apply Zernike minutes on such locales, So copied area in everywhere throughout the picture even in level areas will identified while the procedure time in adequate. At that point works by first applying DWT (Discrete Wavelet Transform) to the information picture to yield a diminished measurement representation[4].

3. RESEARCH GAP

TawakaChihaoui et al. detected the forgery in digital images but could not detect the forgery in digital images having rotation attacks and scaling attack on it. In the proposed system we detect the forgery in the digital images having various attacks on it. Tarman (2017)detected the forgery with rotation attack on maximum rotation angle of 180 degree which is required to be improved for rotation attack more than 180 degree.
Proposed Methodology

SIFT (Improved - Single Invariant feature transform) Algorithm
The I-SIFT algorithm can be to extract robust features which can allow it to discover if a part of an image was copy–moved, besides, which geometrical change was connected. In fact, the copied part has basically the same appearance of the original one, thus key points extracted in the forged region will be quite similar to the original

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

ones. Therefore, matching among I-SIFT features can be adopted for the task of determining possible tampering. the first step consists of I-SIFT feature extraction and key point matching, the second step is devoted to key point clustering and forgery detection, while the third one estimates the occurred geometric transformation, if tampering has been detected.

The proposed approach is based on the I-SIFT algorithm to extract robust features which can allows it to discover if a part of an image was copy-moved and furthermore which geometrical transformation was applied. The proposed system use cluster based approach to detect the forgery in the image. Proposed system works in the following phases:

I-SIFT Algorithms works in following steps :

A. Preprocessing

In this module we need to evacuate if any clamor happened in our info picture. Clamor is only any undesired data that contaminants a picture. Proposed framework utilize Gaussian channel to evacuate the clamors.

B. Feature Extraction

It is a calculation in PC vision to recognize and portray neighborhood includes in pictures. For any article in a picture, intriguing focuses on the item can be separated to give a "highlight depiction" of the article. These highlights depend on shading and surface estimations of the picture. ANN (Artificial Neural Network) and SIFT calculation is utilized to identify shading and Texture.

C. Hierarchical Clustering

Various leveled bunching makes a progressive system of groups which might be spoken to by a tree structure. These groups are separated utilizing the highlights removed in the past stage.

D. Cluster Mean value calculation and comparison

Compute the mean estimations of the bunches and contrast these mean qualities and different groups mean qualities utilizing SIFT Operations. On the off chance that mean estimation of one group is coordinated with the mean estimation of other bunch than procedure the bunches pixel by pixel generally skirt the group to spare the handling time of the framework.

E. Estimate the Geometric Transformation

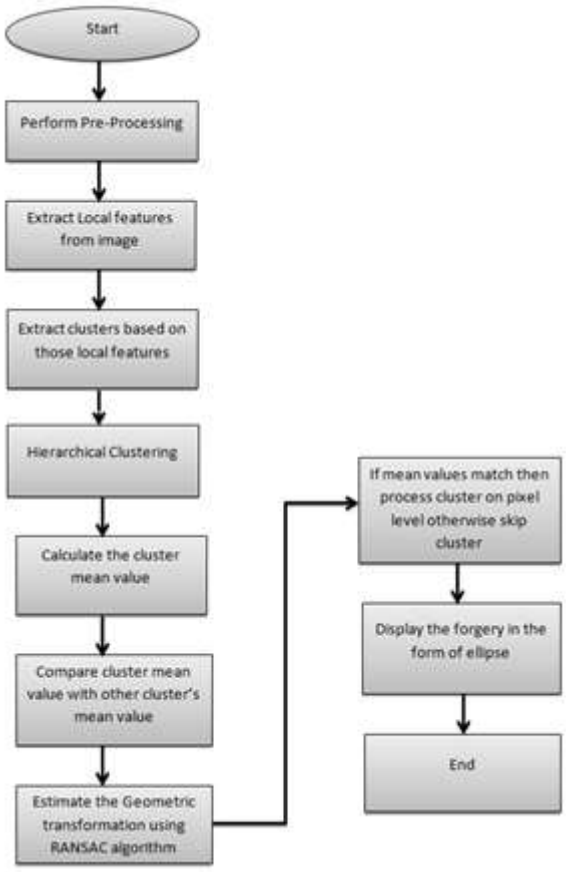
Gauge the geometric changes like pivot, scaling by utilizing RANSAC calculation to recognize the fabrication .

F. Detect Forgery

Figure the absolute number of groups coordinated with alternate bunches by utilizing Multi-SVM Technique and show the coordinating focuses on the picture in type of circles and obscuration.

The proposed algorithm can be represented as following flowchart :

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7



Algorithm to perform hierarchical clustering is explained as below :

RANSAC algorithm can be explained as below:

Step 1: Selects N data items at random.
Step 2: Estimates parameter.
Step 3: Finds how many data items (of M) fit the model with parameter vector within a user given tolerance. Call this K.
Step 4: If K is big enough, accept fit and exit with success.
Step 5: Repeat 1-4 steps L times.
Step 6: Fail if you get here.

4.RESULTS AND DISCUSSIONS

The evaluation of the results gives the performance analysis of the proposed system. Proposed system is tested on various standard dataset as well as real world images. For evaluation of the results of the proposed systems various types of the forgery has been included in the original images.

Proposed System is tested on various input images that contain copy-move forgery in them. Images on which results are calculated on real world images as well as on standard dataset. Following are the results statistics of the proposed system:

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Table No. 1.1 Different combinations of Geometric transformations applied on images of the Proposed dataset.

Attack	Rotation	Scale(x)	Scale(y)
A	0	1	1
B	0	10	10
C	10	20	20
D	90	1	1
E	10	10	10
F	210	1	1
G	30	20	20
H	30	20	20
I	50	20	20

The above table represents the various combinations of attacks comprising of Rotation and Scaling along with image forgery. Rotation attack in the table is specified in the degrees while scaling attack is specified in form of percentage. We have applied the attacks according the values given in the above table to detect the forgery in the given input image. We have defined the various attacks combinations with Alphabets from A to I.

Table 1.2 : Comparison Table of Existing System And Proposed System on basis of various parameters

Parameter	Existing System	Proposed System
Maximum Angle Detected	180 Degree	210 Degree
Scaling	1.5	1.7
Scaling + Rotation	1.5+90	1.6+180
TPR	83.13%	87.43%
FPR	15.23%	11.32%
Accuracy	84%	93%

Above table represents overall results on various parameters like Maximum angle detected, TPR, FPR and accuracy. A comparison on these parameters has been shown in the above table between the existing system and proposed system. It is shown that maximum angle detected by the existing system is 180 degree and that of proposed system is 210 degree. As shown above proposed system shows the improved values of precision. It is also shown that forgery in the existing system cannot detect if rotation angle increases above 180 degree. On the other hand, proposed system shows the accuracy of 93% on these rotation angle values

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Graph representing the accuracy of the proposed system on different attacks

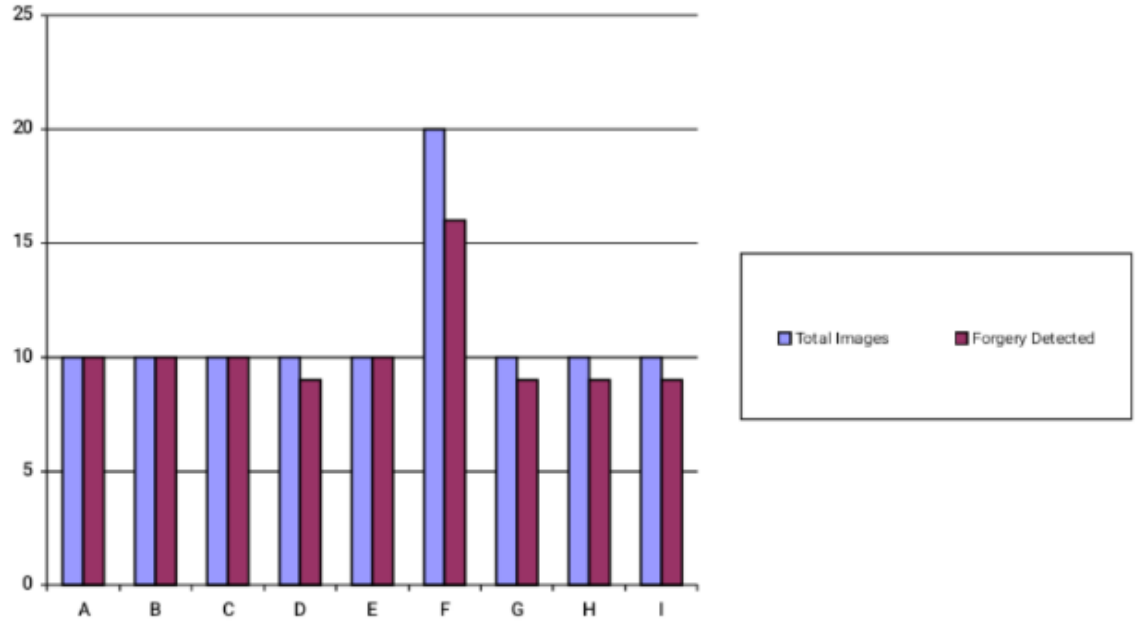


Fig : Graph representing the accuracy of the proposed system on different attacks

4. CONCLUSION AND FUTURE SCOPE

Conclusion

In the proposed work, we have implemented the Improved SIFT (I-SIFT) algorithm to detect the copy move forgery in the digital images. Proposed system is tested on various images of standard dataset. Overall Accuracy of the proposed system is calculated to as 93% which is better than that of existing algorithms. TPR of existing system is 83.13% whereas TPR of proposed system is 87.43% which shows the good results over true positives as compare to existing system. FPR of existing system is 15.23% where as FPR of the proposed system is 11.32% which shows that the proposed system shows the least negative results. It is concluded that the proposed system shows considerably high improvement than the previous systems. In proposed work, we use clusters and their mean values to find the forged area within the image to reduce the overall processing time. Proposed system also shows good accuracy in the images that can contain scaled forgery or forgery with geometric transformations.

Future Scope

In future, system can be enhanced to minimize the processing time to detect the forgery in the images to few seconds or even microseconds. Further the proposed system can also be extended to detect the forgery in the video files by extracting the frames from the video files and apply the proposed techniques to every video frame to detect the forgery in the video files. In future, combinations of more attacks can be tested and enhancements can be made in the proposed systems according to the results.

REFERENCES

[1] S. Thakur,R. Kaur,Dr. R. Chadha,J. Kaur(2016),"A Review Paper on Image Forgery Detection In Image Processing", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. I (Jul.-Aug. 2016), PP 86-89.

[2] Weihai Li, Yuan Yuan, and Nenghai Yu, (2016), “Detecting Copy-Paste Forgery of Jpeg Image via Block Artifact Grid Extraction”, Lnla2008 - Lausanne, Switzerland, The 2008 International Workshop on Local and Non-Local Approximation in Image Processing

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

[3] C. Bhalla, S. Gupta(2016), "A Review on Splicing Image Forgery Detection Techniques",IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555, Vol.6, No.2, Mar-April 2016.
[4] Joshi Chintal J, Prof. Shailendra K Mishra,(2016), "Investigating The Possibility Of Recognizing The Forgery By Using Spatial & Transform Domain", International Journal of Application or Innovation in Engineering & Management, Vol 5, Issue 8.
[5] Sowmya K.N., H.R. Chennamma,(2015), "A Survey on Video Forgery Detection", International Journal of Computer Engineering and Applications, Volume IX, Issue II,pp. 17-27
[6] Nikhilkumar P. Joglekar, Dr. P. N. Chatur ,(2015) "A Compressive Survey on Active and Passive Methods for Image Forgery Detection", International Journal of Engineering & Computer Science, Volume 4 Issue 1.
[7] Hussain MD Abu Nyeem, (2015), "A digital watermarking framework with application to medical image security",Queensland University of Technology, 40th International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2015. 19-24 April 2015, Brisbane, Australia.
[8] Reza Monsefi, HadiSadoghiYazdi, (2014), "Localization of Wireless Devices in Covered Areas using Compressive Sensing", International Journal of Computer Applications (IJCA),Number 7 - Article 6.
[9] Prabhu, GeethuPriya. P, (2014), "Automatic Image Forgery Exposure using Illuminant Measure of Face Region and Random Object Detection Method", International Organization of Scientific Research (IOSR) vol.9 issue.2
[10] Anu George, Suresh BabuV(2014), "Robust image hashing scheme for image forgery detection", Unique Journals Communication (UJC), UJEAS 2014, 02 (02): Page 143-146.
[11] S S.Patil, AN.Patil, N P.Patil, J D.Dhongde, B S.Khade, "Digital Image Forgery Detection Using Basic Manipulations In Facebook", International Journal of Scientific & Technology Research Volume 3, Issue 3, March 2014.
[12] Jessica Fridrich, David Soukal, and Jan Lukas, (2014), "Detection of Copy-Move Forgery in Digital Images", International Journal of Computer Applications 88(8):41-45, February 2014
[13] Ramesh C. Pandey, Sanjay K. Singh, K. K. Shukla and R. Agrawal(2014),"Fast and Robust Passive Copy-Move Forgery Detection Using SURF and SIFT Image Features",2014 9th International Conference on Industrial and Information Systems (ICIIS),IEEE,2014
[14] Fabio Marturana, (2014), "Device classification in digital forensics triage", Faculty of Science Department of Mathematical Sciences, University of Stellenbosch, IEEE International Conference on Communications Workshops (ICC), 676-681, 2014.
[15] Archana V. Mir, Dr S. B. Dhok, Dr N. J. Mistry and Dr P. D. Porey, (2013), "Catalogue of Digital Image Forgery Detection Techniques, an Overview", Proc. of Int. Conf. on Advances in Information Technology and Mobile Communication, Elsevier,2013
[16] S. A.Thajeel and G. 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.
[17] Paolo Bestagini, Simone Milani, Marco Tagliasacchi, Stefano Tubaro, "Local tampering detection in video sequences",(2013),MMSP'13, Sept. 30 - Oct. 2, 2013, Pula (Sardinia), Italy
[18] Bin YANG, Xingming SUN , Xianyi CHEN ,(2013), Jianjun ZHANG , Xu LI , "An Efficient Forensic Method for Copy–move Forgery Detection Based on DWT-FWHT", Journal of Advances in Information Technology;Nov2013, Vol. 22 Issue 4, p1098.
[19] K.Karthikeyan and R.Sowmya Lakshmi,(2013), "Fuzzy based Image Forgery Localization Using Blocking Artifacts", Institute of Research In Engineering and Technology (IRET),2013.
[20] Leida Li, Shushang Li, Hancheng Zhu,(2013), "An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns", Journal of Information Hiding and Multimedia Signal Processing, Volume 4, Number 1
[21] F. Battisti, M. Carli, A. Neri,(2012), "Image forgery detection by using No-Reference quality metrics", Proc. SPIE 8303, Media Watermarking, Security, and Forensics 2012,Vol. 8303
[22] Roman-Gonzalez, K. Asalde-Alvarez,(2012) "Image Processing by Compression: An Overview" ,Proceedings of the World Congress on Engineering and Computer Science 2012 Vol I..