DIGITAL FORGERY DETECTION USING MODIFIED LBP TECHNIQUE

[1]*Tanvi Sharma*, [2]*S. R. Tandan*, [3]*Sunil Sharma*

[1,2,3]*Department of Computer Science and Engineering,*
Dr C V Raman University,
Bilaspur, Chhattisgarh 495001, India

Abstract

The technical evolution of the world, and win the confidence and trust in the digital image processing technology is apart of the game. In everyday life, people come across forged, fake or counterfeit paintings from normal magazines to the business sphere. In addition, In the media, scientific journals, political campaigns, courtrooms, and the photo hoaxes that end up in our inboxes, fake, images will appear more and more often, in a unique way, in order to identify a forged or fake image to the required degree of complexity. The tempering of the image from the point of view of a digital work can be seen as a creative work, but there are some cases in which the forged frames have been intentionally abused. This is a critical situation occurs when one of the images will be shown as a proof of the medical reports of crimes, etc., where you have a fake image, it leads to the death of the patient, and for the criminal to get away. Tempering of the original image, leading to the illegal distribution. In this research we are using local binary pattern to detect whether given image is forged. We have also compare our work with different techniques which were done in past years. We have compared various parameters to see how efficient our work is with respect to other techniques.

Keywords: - Forgery, re-touching, slicing, morphing, copy-move, LBP.

I.INTRODUCTION

Forgery was defined as a crime, it is incorrect, change, or edit a document in order to deceive other people. This may involve the production of a forged document, or spurious entities. However, We live in a digital age, where digital technology has become the dominant technology for the production, processing, storage, transfer and storage of your information. Digital forgery is incorrectly modification the digital content, such as photos, images, documents, music, and for economic gain. This may be a fraud, and identity theft. Most of the digital and counterfeits act because digital images are often drawn to the attention of the viewers. And with the widespread availability of strong, the powerful image-processing software(such as Adobe Photoshop, Adobe Premiere, Corel Draw, or GIMP) you can change nearly everything in the picture. For example, photographs of a child (child pornography), activities in the express sexual harassment can be made with simple images, or even without the participation of a real child. Digital techniques are known to be more accurate than standard windows tools, as each of the a portion of the frame can be changed, pixel, one pixel at a time. It's hard for people to find a images crafted in a specific way. Thus, the phrase "show, don't tell" isn't really in the digital age.

II. FORGERY

The computerized picture has gotten quite possibly the main methods for sending and accepting data. It is the premier wellspring of proof for any occasion in the courtroom. It is additionally utilized in legal sciences examinations, military, clinical records, protection, and different fields.

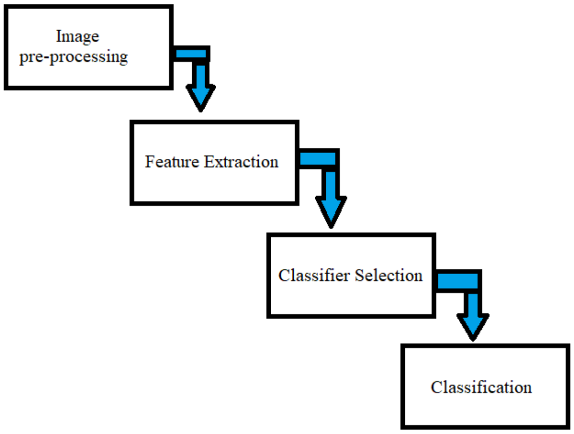


Fig 1: Common structure of image forgery detection

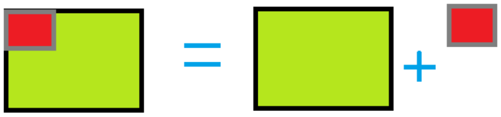
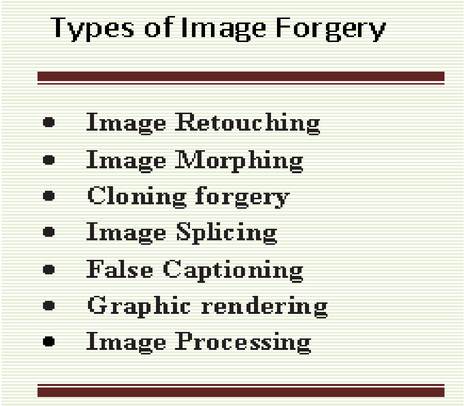


Fig 2: Forged Image = Original Image + Fake Image

Types of Image Forgery: There are three kinds of picture imitation: image retouching, splicing forgery, copy-move image forgery. They are delineated in Figure 1. Notwithstanding the camera used to take pictures, image retouching can be utilized to dispose of any defects later on. Modifying controls the picture by changing its highlights without making observable alterations of the substance. Splicing (for example copy paste) is a type of photographic altering wherein there is advanced joining of at least two pictures into a solitary composite. Maybe the most widely recognized kind of forgeries is the copy-move (for example cloning) forgery. In this forgery type, a piece of the actual picture is reordered into another piece of similar picture with the point of hiding certain highlights in the first pictures.



Types of Image Forgery

- Image Retouching
- Image Morphing
- Cloning forgery
- Image Splicing
- False Captioning
- Graphic rendering
- Image Processing

Fig 3: types of image forgery

Image Splicing: Image splicing forgery is a phenomenon that is just cut-paste a portion of an image with the same or a different source images. If source image is different it may be seen by naked eyes. Image splicing forgery of images makes a radical change in the visual information, as compared with the other forging techniques.

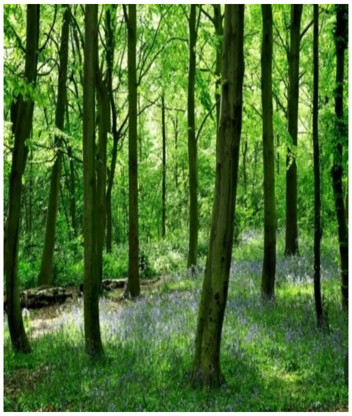


Fig 4: Image of jungle

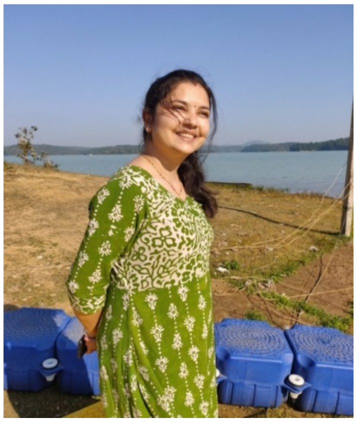


Fig 5: image of woman standing in a river bank

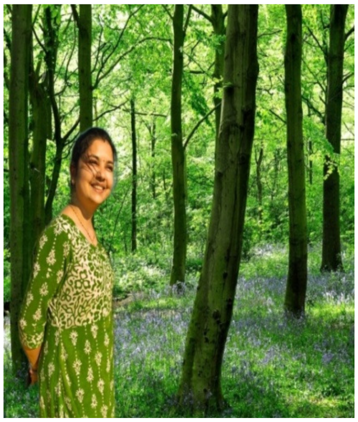
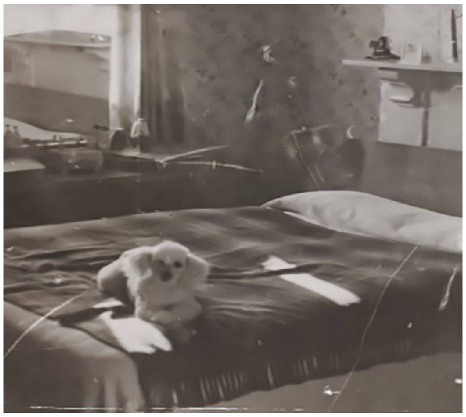


Fig 6: Image Slicing

Image Retouching image retouching is the art and science of image processing, in which the content of a visual image that is enhanced by performing multiple transformations with the help of the available image-editing software. The re-touching of the Picture is mainly made up by all the dominant photographers and improve the function of the digital image, as well as to restore the function of the digital image. Photo retouching is one of the techniques that will be used for the beauty of the image, the features and behavior of a digital image of authenticity, to give it a natural look



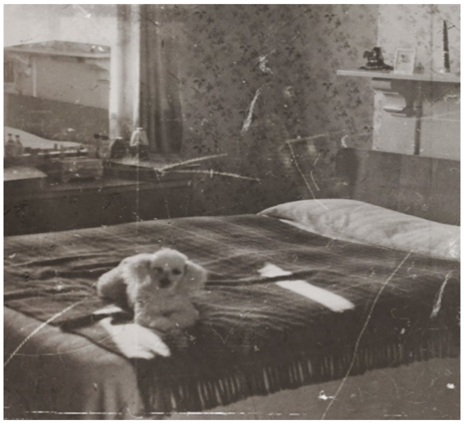
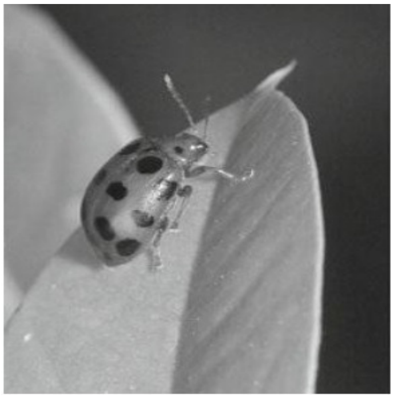


Fig 7: Image Retouching: Tampered image Fig 8: Image Retouching: Original Image

Copy-Move Forgery Copy-move forgery is a widely-used method for tempering the images that will be used for working with digital content in the image. This is the type of image tampering, where a field is to be copied and pasted into another in the same image frame, or hidden, or to create a clone of an object in the frame several times. When tempering a digital image of it's a direct copy of a portion or the part from the digital image, and then paste it into the same frame with a different region



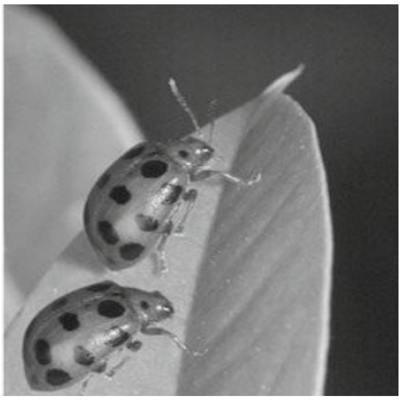


Fig 9: Copy Move: Original Image Fig 10: Copy Move Tampered Image

Image Morphing Morphing is equipped with a power-on process of the transformation of a picture into another picture with a continuous processing of the image. Application combines all the components of an image, i.e., the geometry, and the color of the elements is a lot of different images. The image transformation is most often used by the designers for the creation of an interface between two different styles, modern, digital, font design.

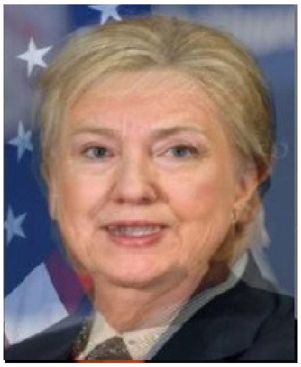


Fig 11: Image Morphing Original Image Fig 12: Image Morphing Original Image Fig 13: Image Morphing Morphed Image

III. PROPOSED WORK

The proposed methodology will deal with image forgery since image is frequently employed method in the domain of image forgery. Algorithm of the local binary pattern forgery detection

```
Start
Input image 1
Crop region
Calculate LBP1 pattern of crop image Ic
Freq_count =0
For i=0 to Width (Ic)
For J=1 to Height (Ic)
Crop image
Iseg =(I (IcWidth, Ic Height))
Calculate LBP of Iseg
If LBP1 == LBPI seg
Freq_count ++
End
End
End
If freq_count>=2
Msg ("Forged image")
End
If freq_count<2
Msg ("Original image")
End
Stop
```

IV. COMPARITIVE RESULT ANALYSIS

Table No 1: Comparative study of different image forgery detection techniques

Sr.no	Paper	Technique	Detection Domain	Advantage	Limitation
1	Splicing Image Forgery Detection Based on DCT and Local Binary Pattern [3]	LBP, DCT, SVM	Image Splicing Forgery	Attained 97% accuracy with chrominance color space	Less accurate in gray and color channel
2	An Integrated Technique for Splicing and Copy-move Forgery Image Detection [4]	DCT, SURF	Spliced Image and Copy-move Forgery	Successfully localized multiple forged region in the same image	Restricted to specific image format like JPEG
3	Image Splicing Detection with Local Illumination Estimation [5]	Local Illumination Estimation, color inconstancy.	Spliced Image	robust over two datasets with good accuracy	Need of human intervention
4	A Forensic Method for Detecting Image Forgery [6]	Code-book, Hash	Spliced image and copy-move image forgery	Generated less complex Codebook with good accuracy	Requirement of source image for splicing detection
5	Detection of Copy-Move Forgery of Images Using Discrete Wavelet Transform [7]	DWT, shift vector	copy-move image forgery	lower computational complexity and detect small size and multiple copy-move forgery	---------------------
6	Detection of Digital Image Forgery using Wavelet Decomposition and Outline Analysis [8]	DCT, Wavelet decomposition	Spliced Image and Copy-move Forgery	Good accuracy with 81.50%	--------------------
7	Image splicing detection based on inter-scale 2D joint	DWT, PCA, SVM	Splicing forgery detection based on	Attained accuracy 96.2 % for the Columbia	Less accurate with color image and better
	characteristic function moments in wavelet domain [9]		inter-scale 2D joint characteristic function	image splicing detection evaluation dataset.	accuracy with gray image.
8	An Effective Algorithm of Image Splicing Detection [10]	Multi-size Block Discrete Cosine Transform (MBDCT), SVM, Image quality metrics (IQMs)	Spliced Image	acquired highest accuracy rate 89.16%	required 80% training for higher accuracy
9	Effective Image Splicing Detection Based on Image Chroma [11]	Gray level co-occurrence matrix (GLCM), SVM	Gray level co-occurrence matrix used for splicing detection	Shown 96.2% of accuracy over the Columbia Image Dataset	----------------------
10	Pixel Based Digital Image Forgery Detection Techniques [12]	DWT	Copy-move Forgery detection	Robust against rotation	considers only 90 , 180 , 270 angle orientation
11	Fast, automatic and fine- grained tampered JPEG image detection via Discrete Cosine Transform coefficient analysis [19]	DCT	Double quantization effects hidden among histograms of DCT coefficients	Insensitive to the tampering methods	restricted to Image Format
12	**Proposed work**	**LBP**	**Image Forgery Detection based on Local Binary**	**High accuracy almost 100% (as parameter is set to 100%) irrespective of image color.**	**Time complexity is high for big dimension images**

V. CONCLUSION

Through advances in innovation and availability, we presently have a progressive chance to improve learning, inventiveness and development, and to contact new crowds around the world, through the multiplication and sharing of show-stoppers and social legacy ('Works').

Moreover, advanced innovations can empower us to record, report and, in certain occasions, reproduce Works that are compromised by ecological dangers, clashes, psychological warfare, quick monetary turn of events, mass the travel industry, burglaries and other regular and human-made debacles ('Endangered Works') or that have been lost.

References

[1] Sudarshan Nelatury, "DIGITAL FORGERY" https://www.researchgate.net/publication/327022702, May 2017

[2] S. Math and R. C. Tripathi, “Digital forgeries: Problems and challenges,” *International Journal of Computer Applications*, vol. 5, no. 12, August 2010, pp. 9-12

[3] J. A. Silversmith, “Photographic evidence, naked children, and dead celebrities: Digital forgery and the law,” Harvard Law School, 1998.

[4] P. Nampoothiri and N. Sugitha, “Digital image forgery - A threaten to digital Forensics,” *Proceedings of International Conference on Circuit, Power and Computing Technologies*, 2016.

[5] J. Fridrich, D. Soukal, and J. Lukáš, “Detection of copy-move forgery in digital images,” *Proceedings of Digital Forensic Research Workshop*, 2003.

[6] Roy A. Huber & A.M. Headrick, *Handwriting Identification: Facts and Fundamentals*, Washington D.C., 2000.

[7] Ron N. Morris*, Forensic Handwriting Identification: Fundamental Concepts and rinciples*, Academic Press, London, 2000.

[8] Katherine M. Koppenhaver, CDE, *Forensic Document Examination: Principles and Practise*, New Jersey, 2007.

[9] B.R. Sharma, Forensic Science in Criminal Investigation and Trials, 4th edn., New Delhi, 2005.

[10] Albert S. Osborn, Questioned Documents, 2nd edn., Delhi,1998

[11] Ordway Hilton, Scientific Examination of Questioned Document, New York, 1982

[12] Wilson R. Harrison, Suspect Documents: Their Scientific Examination, Delhi, rpt, 2001

[13] Ellen David: Questioned Documents: Scientific Examination, Taylor & Francis Washington, 1991

[14] Jan Seaman Kelly & Brian S. Lindblom, Scientific Examination of Questioned Document, 2nd edn., Taylor & Francis Group, London, 2006.

[15] R.E. Jacobson, S.F. Rar, G.G. Attridge, N.R. Oxford, The Manual of Photography

[16] Photography and Digital Imaging, 9th edn., 2000.

[17] Roy A. Huber & A.M. Headrick, Handwriting Identification: Facts and Fundamentals, Washington D.C., 2000