International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.03, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

DWT and PCA Techniques with SURF for Copy-Move Forgery Detection

Nisha Gupta[1], Rajiv Jain[2], Monica Goyal[3]

1 Assistant Professor, SBSSTC Ferozepur, Punjab, (India)

2 Assistant Professor, MIMIT Malout, Punjab, (India)

ABSTRACT

Throughout the most recent couple of years, there has been a developing assemblage of work on apparatuses for computerized picture crime scene investigation. These apparatuses are fit for recognizing altering in pictures from any camera, without depending on watermarks or specific equipment. Rather than watermarks, these apparatuses accept that pictures have certain regularities that are aggravated by altering. So to evaluate the algorithms for image manipulation and to group they based upon their degree of manipulation. It is also important to consider image compression of image files in the area of work. An evaluation and comparison of the existing forgery detection techniques, and carry out the evaluation along with defining a new grouping structure for forgery detection techniques. There are situations when it is hard to recognize the altered district from the first picture. Discovery of fraud part of a picture drives a need of a genuineness and to keep up trustworthiness of a picture. Here in this paper, two techniques such DWT and PCA with SURF as detector, is implemented to detect the forged part of an image from tampered image. Both algorithms have their own validation but PCA with Surf improves to be better in all respective. As in PCA-SURF we can detect as well remove the forged object and it also takes less time to solve the detection problem than DWT-SURF.

Keywords - SURF, PCA, DWT, tampering, forged.

I.INTRODUCTION

A computerized picture is a numeric portrayal of a two-dimensional picture. Contingent upon whether the picture determination is settled, it might be of vector or raster compose. Without capabilities, the expression "computerized picture" as a rule alludes to raster pictures, likewise called bitmap pictures. When we see a photo on our screen or utilize our computerized camera (or scanner), the picture we are survey or managing isn't consistent like a pencil drawing – it is comprised of numerous little components by each other. When we have enough components, we get the fantasy of a photo or picture. Early computerized pictures (previously shading) showed up in highly contrasting. The minor components that contained computerized pictures were either dark or white. These two 'hues' compared to 1 and 0 called bits or binary digits. Digits 1 and 0 are utilized as a part of the twofold (base 2) framework. In this way, a guide (design) made up of these 1's and 0's was alluded to as a bit-outline. Every single computerized picture is a rectangle or square. Today, the components are called pixels.

Crime scene investigation implies the utilization of science and innovation in the examination and foundation of actualities. So the photos or different pictures can be transmitted to and reconverted into pictures by another PC. Computerized criminology (once in a while known as advanced legal science) is a branch of measurable science incorporating the recuperation and examination of material found in advanced gadgets. As advanced picture legal sciences goes for approving the validness of pictures by recouping data about their history. Two principle issues are tended to: the recognizable proof of the imaging gadget that caught the picture, and the identification of hints of falsifications. Now a days, because of the promising outcomes achieved by early examinations and to the continually developing number of uses, advanced picture legal sciences speaks to an engaging examination space for some specialists. With the across the board accessibility of picture altering programming, advanced pictures have been winding up simple to control and alter notwithstanding for non-proficient clients. Picture control has turned out to be typical with developing simple access to effective registering capacities. Some normal picture control with the intension of misdirecting a watcher incorporates:-

- Reorder
- Synthesis or Splicing
- Correcting, recuperating, cloning
- Content implanting or Steganography

Nowadays, due to rapid advances and availabilities of powerful image processing software, modifying the content of digital images becomes much easier with the help of sophisticated software such as Adobe Photoshop. Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners. There are several characteristic of watermarked image:

- Robustness
- Perceptibility
- Capacity
- Embedding method

There are many ways to categorize the image tampering, and generally, we can tell that some usually performed tasks in picture altering are:

- Erasing or concealing an area in the picture.
- Including another protest into the picture
- Distorting the picture data

To insert and splicing image part of the original image is the one of the most typical method. Watermarking is the popular way to counterfeit the forgery image. The digital watermark, unlike the printed visible stamp watermark, is designed to be invisible to viewers. The bits embedded into an image are scattered all around to avoid identification or modification. Therefore, a digital watermark must be robust enough to survive the detection, compression, and operations that are applied on.

II.LITERATURE SURVEY

A proficient and consistent detection method such as DCT proposed by Jessica Fridrich [1] successfully detected the copied area which it merged with the background, even after enhancing or retouching and also even when the forged image is saved in a lossy format, such as JPEG.A novel technique based on transform-invariant features is proposed by P. Kakar and N. Sudha [2].Using the features from the MPEG-7 image signature tools, the transform-invariant features are obtained. The proposed technique detects copy-paste forgeries, with translation, scaling, Also it is efficient for lossy compression, rotation and flipping. This technique gives very high accuracy across post processing operations, and also the cloned regions are found with a high true positive rate and lower false positive rate. Tushant A. Kohale, and P. R. Lakhe [3] studied the combination of block-based and feature based methods, the effect of different types of tampering on the digital image, detect image forgery by copy-move under many types of attacks and accurately locating the duplicated region. Salma Amtullah, and Ajay Koul [4] presented the passive image forensic method based on SURF to detect copy-move forgery in digital images.In this method the features are extracted and their descriptors are obtained by SURF algorithm and the Nearest Neighbor approach is used for feature matching to identify the copy-move forgery in digital images. SIFT techniques are quite effective in producing an attacked image with very few (or no) keypoints, but at the expense of an image distortion. I. Amerini et al [6] evaluated the effectiveness of the attacking methods with respect to perceptual image quality. Based on a perceptual metric, they proposed a modified SIFT keypoint removal method and well supported it with series of perceptive experiments. Mohammad Farukh Hashmi et al [7] proposed a series of algorithms in which the combination of speeded-up robust feature transforms and Wavelet Transforms are used. The authors also showed that their algorithm showed better results in terms of computational complexity and invariance to scale and also for the combination of attacks and rotation. Ramesh Chand Pandey et al [8], used both SURF and SIFT method, to make it very fast and robust in detecting copy-moved regions which are copy-moved with the help of geometrical and illumination transform. Takwa Chihaoui et al [9], proposed a method using the Scale Invariant Feature Transform (SIFT) and Singular Value Decomposition (SVD) method which detects duplicated regions in the same image automatically. The results of hybrid method are robust to geometrical transformations and are able to detect with high performance duplicated regions. Rutuja Tendulkar and Manoj Sabnis [10] here alluded to confirmation of a picture got from communication network a testing as well as necessary task.In this paper, using transform domain, an algorithm to find copy-move forgery is proposed. Fast Fourier Transform (FFT) and Discrete Wavelet Transform (DWT) are applied on a forged picture to discover matching blocks. Sushama Kishor Bhandare [11] reviewed the forensic methods for detecting globally and locally applied contrast enhancement, cut-and-paste forgery, histogram equalization, and noise in the digital image.

III.METHODOLOGY

The Proposed method of copy-move forgery detection has following main parts.

1. Discrete Wavelet Transform

2. Lexicographic Sorting

3. Shift Vector Calculation

4. Neighbor block matching

This method will work as follows:-

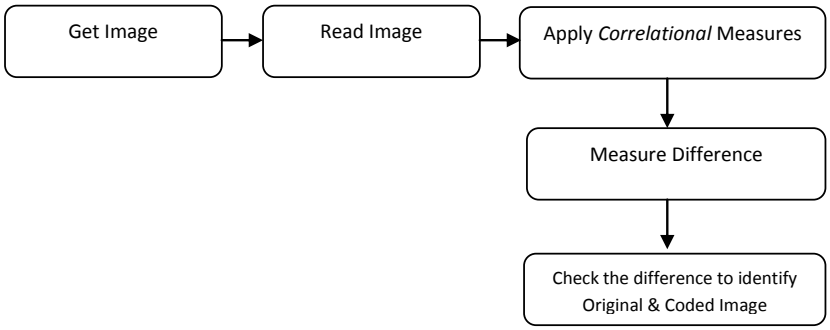

Figure 1: Flow chart to define the methodology

IV.RESULTS

In Matlab, outcome of detecting of the copy pasted part after implementing is shown in below figures. Figure 2 to 6demonstrates the DWT results. Figure 2, shows the original image. Figure 3 below demonstrates the processed input image, after decomposed and output image after all processing.

Figure 2: DWT Original Image

Figure 3: Processed and decomposed DWT Image

Figure 4 demonstrates the image with different color intensity of RGB which is decomposed further in LL of level. Figure 5 demonstrates the original image with 2d color and that image after decomposition in gray scale image. Figure 6, shows the original image with the Decompositon level which have been given as for compression as compressesd decomposited image is demonstrated.

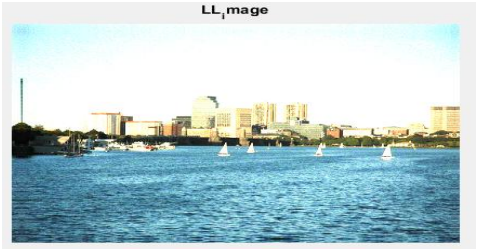

Figure 4: LL color intensity DWT image

Figure 5: 2D color and decomposed Garyscale DWT image

Figure 6: Original and decomposed DWT image

Figure 7: SURF image after detecting copied part

Figure 7, demonstratesthe SURF techniques in which copied part of images is detected from forged image.In MATLAB, outcome of detecting of the copy pasted part after implementing is shown in figures. Figure 8a and 8b demonstrates the DWT-SURF results. Figure 8a demonstrates original image. Figure 8b, demonstrates the detection of copied part from forged image by using DWT-SURF techniques

International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.03, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Figure 8a: DWT-SURF Original Forged Image &Figure 8b: DWT-SURF after Detecting PCA

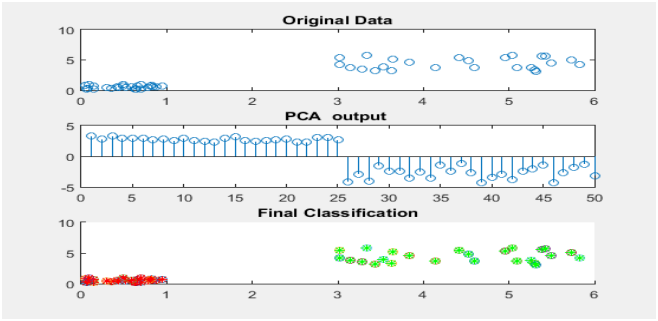

Figure 9: PCA Forged Image with parameter detection

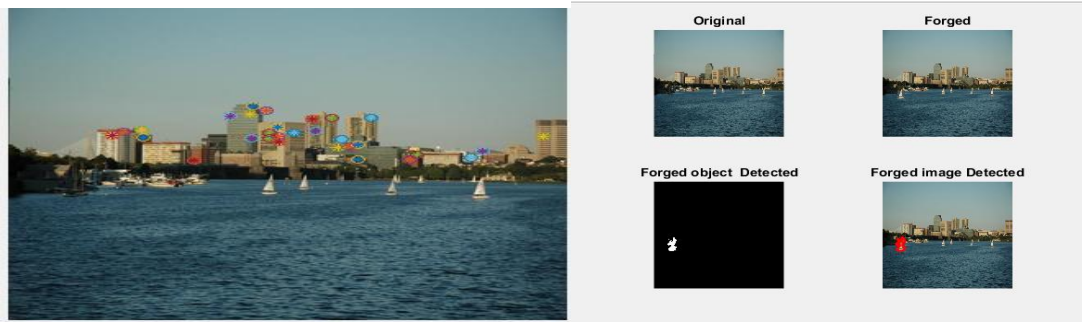

Figure 10a: PCA-SURF Detected Image&Figure 10b:PCA-SURF detecting copied part of Forged Image

Figure 9 demonstrates the performance parameters by utilizing PCA method. Figure10a demonstrates the performance parameters by utilizing PCA-SURF method. Figure 10b demonstrates the detection part of copied in forged image using PCA-SURF method. In above window four sections are demonstrated, initial picture is the original image, second demonstrates the Forged image. Lower initial image demonstrates the actually detected part from black and white image with 2D color. At last, copied part is demonstrated from the forged image.

Table 1: Outcome compared by Elapsed Time (PCA-SURF and DWT-SURF)

Images/ Techniques	PCA-SURF	DWT-SURF

	**2.2387**	**16.8390**
	**4.6027**	**14.3953**
	**3.4736**	**15.1943**
	**3.2826**	**17.0797**

V.CONCLUSIONS

Digital image forensics goes for approving the validness of pictures by recouping data about their history. Duplicate glue imitation, where in a district from a picture is supplanted with another locality from a similar picture (with conceivable changes). Since the replicated part originate from a similar picture, its essential properties, for example, clamor, shading palette and surface, will be perfect with whatever remains of the picture and in this manner will be more hard to recognize and identify these parts. Computerized picture crime scene investigation is a fresh out of the box new research field which goes for approving the genuineness of pictures by recuperating data about their history. In this all the above images having red part using PCA-SURF technique is the detecting copied and pasted part from the original images. Same way DWT-SURF technique is used from above images shows through lines what, from, where, which part has been copied. Both techniques use their own way for detection but as comparing we can say that PCA-SURF is best detection technique as it detect the object and also remove that part where as DWT-SURF does not remove the detected part but only tells that from where the part has been copied. From Table1, it is clarified that PCA-SURF is best as it take half or less time compared to DWT-SURF and results in more clarity of detecting of copied object.The key issues which inquire about found in the writing can be classified into the characteristic, phony recognition, stream mapping, and source distinguishing proof. In this manner, the inventiveness and realness of pictures or information uses much of the time as ending up in testing issue. Analysts have related the common issues to the progress in PC designs, movement, interactive media in the relationship of high processing machines, calculations, expands the many-sided quality of the issue.In response to this, researchers have begun developing digital forensic techniques capable of identifying digital forgeries. These forensic techniques operate by

detecting imperceptible traces left by editing operations in digital multimedia content. In this dissertation, we propose several new digital forensic techniques to detect evidence of editing in digital multimedia content. We use DWT and PCA with SURF for forensic tasks such as identifying cut-and-paste forgeries from compressed images. Additionally, we consider the problem of multimedia security from the forger's point of view. PCA-SURF is best compared to DWT-SURF in tme and Clarity of detecting objects.

REFERENCES

[1] Fridrich. J, "Detection of copy-move forgery in digital images", Digital Forensic Research Workshop, Cleveland, OH, 2003

[2] P. Kakar and N. Sudha "Exposing Post processed Copy-Paste Forgeries through Transform-Invariant Features", vol. 206, no. 1-3, pp. 178–184, 2011.

[3] Tushant A. Kohale, and P. R. Lakhe " Detection of Post operated Copy Move Image Forgery by Integrating Block Based and Feature Based Method", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014

[4] Salma Amtullah, Ajay Koul "Passive Image Forensic Method to detect Copy Move Forgery in Digital Images" IOSR Journal of Computer Engineering Volume 16, Issue 2, Ver. XII pp 96-104 March 2014

[5] Andrea Costanzo, Irene Amerini, Roberto Caldelli, "Forensic Analysis of SIFT Key point Removal and Injection," in IEEE Transactions On Information Forensics And Security, VOL. 9, NO. 9, September 2014.

[6] Amerini, F. Battisti, R. Caldelli, M. Carli and A. Costanzo, "Exploiting perceptual quality issues in countering SIFT-based Forensic methods," 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Florence, 2014, pp. 2664-2668.

[7] Mohammad Farukh Hashmi, Vijay Anand, Avinash G. Keskar "A Copy-move Image Forgery Detection Based on Speeded Up Robust Feature Transform and Wavelet Transforms" 5th International Conference on Computer and Communication Technology, 2014.

[8] R. C. Pandey, S. K. Singh, K. K. Shukla, R. Agrawal, "Fast and robust passive copy-move forgery detection using SURF and SIFT image features," 9thInternational Conference on Industrial and Information Systems (ICIIS), Gwalior, pp. 1-6. 2014.

[9] Takwa Chihaoui, Sami Bourouis, and Kamel Hamrouni, "Copy-Move Image Forgery Detection Based On Sift Descriptors And Svd-Matching," in 1st International Conference on Advanced Technologies for Signal and Image Processing - ATSIP'2014, March 17-19, 2014, Sousse, Tunisia

[10] Rutuja Tendulkar and Manoj Sabnis "Copy-Move Image Forgery Detection Using Transform Domain", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, May 2015.

[11] Sushama Kishor Bhandare, Nitin Krishnarao Bhil, "Digital Image Forensic", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 7, July 2015.