IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005293 |

Identification of Copy Move Forgery Detection in Digital Images

M Sai Krishna[1], M Srikanth[2], M Anirudh[3], M Sanjay[4]

UG Students, Dept. of Electronics and Communication Engineering, Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India[1-4]

ABSTRACT: ABSTRACT: In this rapidly evolving digital world, it has become increasingly difficult to distinguish between an original image and a manipulated image. New tools, which are technologically advanced and are easily accessible, are being used to modify an image to meet one's sinister purposes. Rampant counterfeiting of images has been used to create distrust among people. This necessitates the need for forensic digital analysis of images. This project proposes a method for the verification of images. This method is used to detect the copy move modifications within an image, using the discrete cosine transform. The features that are extracted from these coefficients helps us to obtain transfer vectors, which are clustered and through this it is likely to determine whether copy move forgery is done in an image or not. The test results obtained from benchmark datasets illustrate the effectiveness of the proposed method

KEYWORDS: Copy Move Forgery, Discrete Cosine Transform, Datasets

I. INTRODUCTION

Digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analysing and reporting on data stored electronically. Image forensics aims at validating the authenticity of images by recovering information about their history. Images are easily manipulated. This diminishes credibility of video tapes and images presented as evidence. Doctored images can be used to cause unrest in civil society. Many cases of digital image forgery are present. They are categorized into major groups such as: Image Retouching, Image Splicing, Copy Move Forgery and Morphing. In this paper, the main area of discussion is on Copy move forgery. The existing methods in this methodology is analysed and explained. We have proposed an algorithm in this paper which detects the copy move forgery modifications in a digital image using discrete cosine transform. In a Copy-Move forgery, a part of the image itself is copied and pasted into another part of the same image. This is usually performed with the intention to make an object "disappear" from the image by covering it with a segment copied from another part of the image. Textured areas, such as grass, foliage, gravel, or fabric with irregular patterns, are ideal for this purpose because the copied areas will likely blend with the background and the human eye cannot easily discern any suspicious artifacts. Because the copied parts come from the same image, its noise component, colour palette, dynamic range, and most other important properties will be compatible with the rest of the image and thus will not be detectable using methods that look for incompatibilities in statistical measures in different parts of the image. To make the forgery even harder to detect, one can use the feathered crop or the retouch tool to further mask any traces of the copied-and-moved segments.

II. RELATED WORK

The copy-move technique is another popular method used today for image forgery, where a region of an image is used to hide another region from the same image. The existence of two identical regions is not ordinary in natural images; thus, this property can be used to detect this type of manipulations. Even after applying some post-processing processes, such as edge smoothing, blurring, and adding noise to eliminate visible traces of manipulation, there will be two extremely similar regions in the manipulated image. In the literature a large number of copy-move forgery detection methods have been proposed. Nevertheless, all of these methods can be classified into two main categories: block-based and key point-based methods [1,2] . Of all those, one of the most used to detect copy-move forgery is the method that use a block matching algorithm. In this algorithm, the image is divided into overlapping blocks, and the blocks are compared to find the duplicated region.Fig 2.1 shows a general scheme of a block matching algorithm.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005293 |

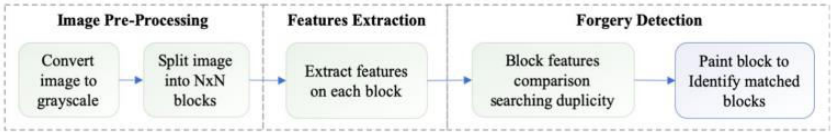

Fig 2.1: General block matching algorithm

Fridrich et al. [3] proposed a method based on the discrete cosine transform (DCT) to identify copy-move forgery. The method split the image into overlapping blocks of 16 * 16. Then, the DCT coefficient characteristics are extracted from each block and then these coefficients are classified lexicographically. After the lexicographical classification, comparable squares are distinguished, and the duplicated regions are found. Fridrich et al. introduced one of the first techniques that use DCT to identify copy-move forgeries on images. Popescu et al. [4] introduced a technique to recognize duplicate regions within images. Popescu's algorithm employs principal components analysis (PCA) rather than DCT. The algorithm uses PCA on small fixed-size image blocks, and then each block is lexicographically ordered. This method has proved great efficiency to recognize copy move forgeries. Kang et al. [5] used singular value decomposition SVD to distinguish the modified areas in a picture. By applying SVD, a feature vector is extracted, and the dimensions reduced. Then, identical blocks were identified by the use of a lexicographic classification. Kang's method demonstrated to be robust and effective. The results of the experiment prove the efficacy of the method.

Huang et al. [6] introduced a method to identify copy move manipulation over digital images applying SIFT algorithm. The authors showed the SIFT calculation algorithm using the block matching function. This method gives great results even when the image is noisy or compressed. In Bo X et al. [7], a scheme based on speeded up robust features (SURF) was proposed, which have key point characteristics better than SIFT because they work better with post processing techniques such as brightness and blur variations. However, the methods based on key points present a problem of visual output because the copied and pasted regions consist of lines and points that do not show a clear and intuitive visual effect. Amerini et al. [8], proposed a method based on SIFT. The proposed method can identify copied regions in images. Also, the method proposed can detect which geometric transformation was applied. Due to the copied region of the image looks the same as the original, the key points extracted in the duplicated region will be identical to those in the original. This method is also useful with low-quality factor compressed images.

III. PROPOSED ALGORITHM

In this work, an improved algorithm for copy-move forgery detection is proposed. The algorithm is based on the technique introduced by Fridrich [3]. A diagram presenting the main processes of the detection algorithm can be found in the Fig 3.1.

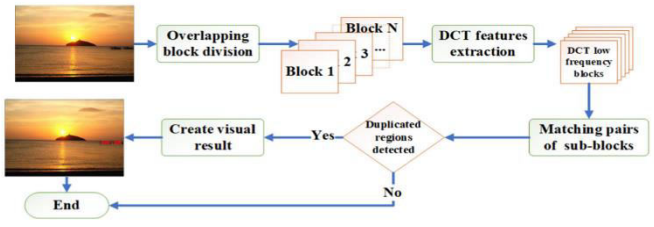

Fig 3.1: Flowchart of Detection algorithm

The algorithm has been explained in the form of a summary as shown in the Fig 3.2:

- Divide the image into small overlapping blocks of size B*B from top-left to bottom-right
- Compute the DCT transformation of every block, sort the coefficients in a zig-zag fashion and truncate the list to contain the first k elements.
- Make a lexicographic sort of the truncated coefficient lists, and for each list, compute a similitude measure between its nearest neighbors. If the similarity is lower than the threshold, blocks are considered as identical.

For every pair of identical blocks, the translation vector is computed. If the number of vectors in a given direction exceed a predefined quantity, every block is considered as part of the copy-move tampering. The block size and

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005293 |

thresholds chosen for the algorithm should be dependent mainly on the size of the image and the expected size of the modification.

IV. PSEUDO CODE

The pseudo code for matching the blocks in the image is shown below:

```
for i = 1,.....,k do
    if sort_block_i1 = sort_block_(i+1)1 then
            p1 <- sort_block_i0
            p2 <- sort_block_(i+1)0
            s <- vectornorm(p1 - p2)
            s_v_c[s] <- s_v_c[s]+1
            m_b.add([sort_block_i1 , sort_block_(i+1)1 , p1,p2,s)
```

m_b refers to the matched blocks. s_v_c and shift_vector_count are used to store the shift vector count of the two blocks. i is a variable used to iterate through the loops. Sort_block is the variable where the dct coefficients are stored after they are sorted lexicographically.

V. SIMULATION RESULTS

The necessary tools needed to execute this project is listed and explained in this chapter. The system requirements are as follows:

- Visual Studio Code
- Python 3
- Operating System : Windows
- Numpy
- Scipy
- Open CV(CV2)
- Matplotlib

The datasets required to perform the proposed method are explained briefly. The CMFD GRIP Dataset by Cozzolino et al. [10] (hereinafter referred as D1) is a dataset composed by 80 images, with realistic copy-move forgeries. All these images have size 768 * 1024 pixels, while the forgeries have arbitrary shapes, aimed at obtaining visually satisfactory results.

The CoMoFoD database [11] (hereinafter referred as D2) has 260 image sets, 200 images in small image category 512 * 512. Following transformations are applied:

- Translation a copied region is only translated to the new location without performing any transformation
- Rotation a copied region is rotated and translated to the new location
- Scaling a copied region is scaled and translated to the new location The distortion to the dataset's images can be noise adding, image blurring, brightness change, color reduction, contrast adjustments or the combination of two or more distortions on a copied region before moving it to the new location.

Ardizzone et al. [12] make a copy-move forgery dataset (hereinafter referred as D3) which contain a medium sized image, almost all 1000 * 700 or 700 * 1000. This dataset contains 50 not compressed images with simply translated copies and 46 not compressed images with 11 different types of rotation around the angle zero in the range of [-25, 25] with step 5 and 11 scaling factors in the range of [0.75, 1.25] with step 0.05.

The CMH dataset (hereinafter referred as D4) was created by [13] and comprises 108 realistic cloning images. Each image is stored in the PNG format (which does not modify pixel values), and has a resolution varying from 845 * 634 pixels (the smallest) to 1296 * 972 pixels (the biggest).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005293 |

The outputs obtained by executing the code are shown from Fig 5.1 to 5.3.

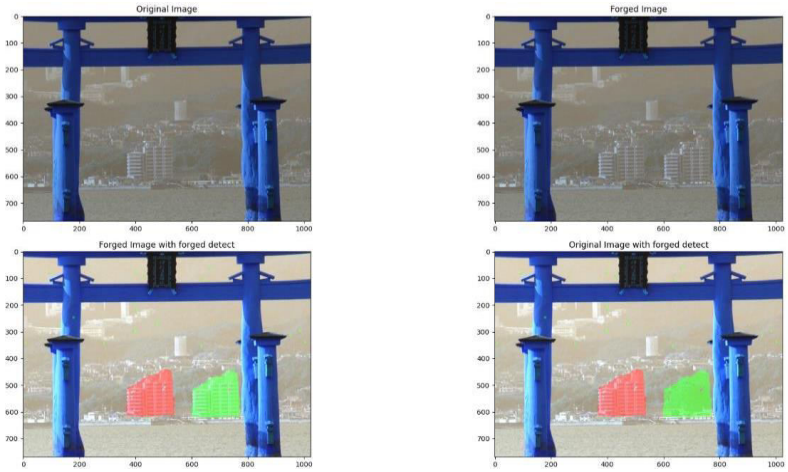

Fig 5.1: Sample Output I

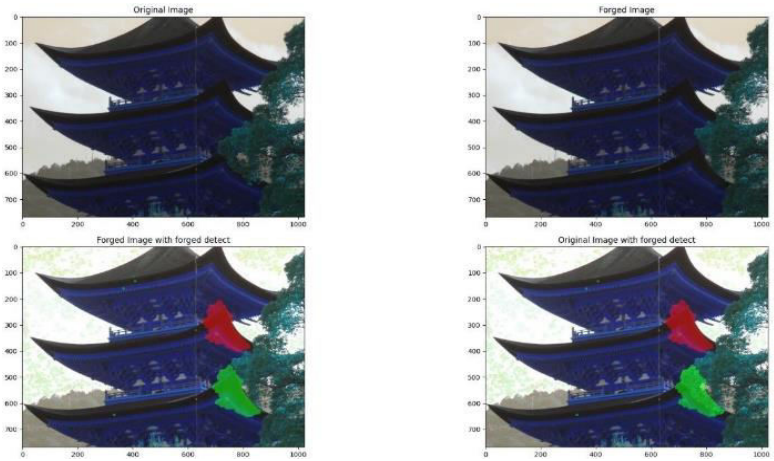

Fig 5.2: Sample Output II

Fig 5.3: Sample Output III

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005293 |

The results summarized in the Table 5.1 shows a high accuracy precision and recall over the three datasets D1, D2 and D3. Our proposed algorithm gets a precision average over the 93% even over images that contain distortion, such as an increase or decrease of brightness and/or contrast, and small geometrical transformations like slight degree rotation.

Table 5.1 Results

Datasets	Precision (%)	Recall (%)	F1 (%)
D1	97.67	58.71	73.33
D2	88.66	57.25	69.57
D3	99.89	81.06	89.43
D4	92.34	60.87	73.37
Average	94.64	64.47	76.42

The proposed method outperformed [14] in terms of average precision.

VI. CONCLUSION AND FUTURE WORK

As at the beginning of this project says the famous saying goes, ‘‘A picture is worth a thousand words’’. Therefore, having faster and reliable algorithms to analyze the integrity of an image is needed. Nowadays, thanks to the fast and easy way to share images plus the easiness of use professional image editing tools make it harder to detect forgeries.

As the world is getting digitalized rapidly, there will be a continuous rise in image forgeries and this algorithm holds great significance.During the development of this work, experiments were performed using the proposed algorithm against six different datasets widely used in the literature. This group of images contained different types of formats, sizes, and additional transformations to the copy-move manipulation.

In this work, an exhaustive study on existing forgery detection techniques has been carried out, emphasizing on copy-move detection. Also, a new approach for forgery detection was presented. The experiments carried out with the proposed algorithm have shown their robustness and efficiency in the results obtained. The algorithm can detect and locate with high precision the duplicate zone in the image.

To validate our results, it is essential to compare our algorithm to a related method, such as the one proposed by Alkawaz et al. [14] in which the authors get a 64.38% of precision using a block size of 8 * 8. Our algorithm showed an average precision of 94.64% compared to 64.38% obtained in [14]. The proposed method outperformed [14] in terms of average precision.

REFERENCES

[1] Park CS, Choeh JY (2018) Fast and robust copy-move forgery detection based on scale-space representation. Multimed Tools Appl 77(13):16795–16811
[2] Teerakanok S, Uehara T (2019) Copy-move forgery detection: a state-of-the-art technical review and analysis. IEEE Access 7:40550–40568. https://doi.org/10.1109/ACCESS.2019.2907316.
[3] 3 Fridrich J, Soukal D, Lukas J (2003) Detection of copy move forgery in digital images. In: Proceedings of the digital forensic research workshop. Binghamton, New York, pp 5–8
[4] Popescu AC, Farid H (2004) Exposing digital forgeries by detecting duplicated image regions. Department of Computer Science, vol 646
[5] Kang X, Wei S (2008) Identifying tampered regions using singular value decomposition in digital image forensics. In: 2008 international conference on computer science and software engineering, vol 3, pp 926–930. https://doi.org/10.1109/CSSE.2008.876
[6] Huang H, Guo W, Zhang Y (2008) Detection of copy-move forgery in digital images using SIFT algorithm. In: 2008 IEEE Pacific-Asia workshop on computational intelligence and industrial application, vol 2, pp 272–276. https://doi.org/10.1109/PACIIA.2008.240

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005293 |

[7] Bo X, Junwen W, Guangjie L, Yuewei D (2010) Image copy-move forgery detection based on SURF. In: 2010 international conference on multimedia information networking and security.Nanjing, China, pp 889–892. https://doi.org/10.1109/MINES.2010.189

[8] Amerini I, Ballan L, Caldelli R, Del Bimbo A, Serra G (2011) A SIFT-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans Inf Forensics Secur6(3):1099–1110

[9] Zhao J, Guo J (2013) Passive forensics for copy-move image forgery using a method based on DCT and SVD. Forensic Sci Int233(1):158–166

[10] Cozzolino D, Poggi G, Verdoliva L (2015) Efficient dense-field copy-move forgery detection. IEEE Trans Inf Forensics Secur10(11):2284–2297

[11] Tralic D, Zupancic I, Grgic S, Grgic M (2013) Comofod–new database for copy-move forgery detection. In: Proceedings ELMAR-2013. IEEE, pp 49–54

[12] Ardizzone E, Bruno A, Mazzola G (2015) Copy-move forgery detection by matching triangles of keypoints. IEEE Trans InfForensics Secur 10(10):2084–2094

[13] Silva E, Carvalho T, Ferreira A, Rocha A (2015) Going deeper into copy-move forgery detection: exploring image telltales via multi-scale analysis and voting processes. J Vis Commune Image Represent 29:16–32

[14] Alkawaz MH, Sulong G, Saba T, Rehman A (2018) Detection of copy-move image forgery based on discrete cosine transform.Neural Comput Appl 30(1):183–192

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details