AN EFFICIENT FORGERY DETECTION IN DIGITAL IMAGES USING MRR TECHNIQUE

S. Irudhaya Ananthi, S. Sophia Rani and K. Rani
Post Graduate Department of Computer Science
Jayaraj Annapackiam College for Women (Autonomous),
Periyakulum, Theni Dist, Tamil Nadu, India
gladisrani.k@gmail.com

Abstract

The identification of image authenticity has received much attention because of the increasing power of image editing methods. This paper proposes a novel forgery detection algorithm to recognize tampered in painting and copy-move images, which is one of the effective approaches for image manipulation. The proposed algorithm contains two major processes: suspicious region detection and forged region identification. Suspicious region detection searches the similarity blocks in an image to find the suspicious regions and uses a similarity vector field to remove the false positives caused by uniform area. Forged region identification applies a new method, multi-region relation (MRR), to identify the forged regions from the suspicious regions. After that Discrete Cosine Transform is applied to the suspicious region and then features are extracted to apply detection algorithm. Finally False alarm removal to fill any holes or to remove the false regions. The experimental results show that the proposed approach has good performance with fast speed under different kinds of in painting and copy-move images.

Key words: *Forgery detection, Multi-region relation, Discrete Cosine Transform, copy-move images.*

1. Introduction

The detection of image authenticity [1–4] is becoming an important research topic because advanced image processing tools can help people make forged images easily. The detection of digital forgery can be classified into active-based [5–7] and passive-based [8–20] approaches. Active-based approaches tract prior inserted information from a digital image (e.g., digital watermarks signatures)to identify the authenticity. If the embedded information is detected to be changed, the image is recognized as a tampered image. In contrast active-based approaches, passive-based approaches detect the feature consistency in a digital image without the embedded information. Region duplication is a common type of forgery. Fridrich et al. [8] detected duplicated regions by matching the discrete cosine transform (DCT) coefficients of overlapping blocks. Langille and Gong [9] used zero normalized cross correlation (ZNCC) as the similarity measurement. Mahdian and Saic[10] applied blur moment invariants to detect duplicated regions.

Huang et al. [11] used a scale invariant feature transform (SIFT) algorithm to extract SIFT descriptors, which describe the correlations between the copy region and the paste region. When an image is forged using the copy-paste method or the matting technique, lighting inconsistency is a good indication of a forged image because the lighting is not consistent over the image. Johnson and Farid[14] described how to estimate the 3-D direction of a light source from the lighting reflection in a human eye. Another one of their methods [15] estimated a low-parameter model for complex lighting environments. Lee et al. [16] proposed a detection method by computing the lighting direction from a segmented image. The corresponding device parameters are not the same when the images are acquired from different acquisition devices. A good indicator for a normal image is the comparison of these parameters because they should be the same between two different areas in an image. Lukas et al. [19] estimated the sensor's pattern noise of the target region and the referred sensor's pattern noise. Then the statistical analysis of regional correlations was used to identify forged regions.

Lin et al. [20] employed a mismatch camera response function to detect image composition. Johnson and Farid used lateral aberration to identify tampered region. When the image was tampered with, the local lateral aberration of the tampered region is inconsistent with the global aberration. Popescu and Farid employed an expectation–maximization (EM) algorithm to quantify specific correlations between the pixels of the image. JPEG images can be re-saved in JPEG format after being manipulated, and the characteristics of double JPEG compression are a good clue for the detection of forged images. Li et al. [12] examined the mismatch information of block artifact grids (BAGs) as evidence of copy-paste forgery. Qu et al. [13] proposed a novel independent component analysis (ICA)-based algorithm to search for areas of double JPEG compression to find image splicing forgeries. Re-sampling is usually used in image composites, such as image resizing, rotation and translation. The interpolation is adopted to generate irregular periodic relations between the pixels of the image. Popescu and Farid [17] introduced an EM algorithm to examine whether or not the image is re-sampled. Mahdian and Saic [18] analysed specific periodic properties for interpolated signals that can be used to detect any re-sampling operation in the image.

The technique of image in painting can be applied to produce a type of forged image. Consequently, the detection of these forged images is becoming an important issue. Wu et al. proposed a detection algorithm that finds the abnormal similarity for all blocks in the image, and then employs a fuzzy membership function to identify in painting regions in the image. Lin et al presented a fast algorithm that analyzes the DCT coefficients of the double quantization effect.

The algorithm is able to detect fine-drained forged regions in the JPEG image. An in painting image is constructed by filling the target area using the surrounding regions in the same image; therefore, the key problem in recognizing the fake region is to search for similar regions in the faked image. However, a non-faked image may have some very similar parts in the background, especially uniform regions such as the sky or sea, which will interfere with the detection process. This paper proposes an effective forgery detection algorithm for in painting forged images. Suspicious region detection searches for similar blocks in an image to find the suspicious regions and uses vector filtering to filter out non-forged regions. Forged region identification applies a multi-region relation (MRR) technique to recognize the forged region.

MRR can effectively remove some suspicious regions from a uniform region. The technique has improved the recognition accuracy for the images containing a uniform background. Moreover, we propose a two-stage searching algorithm based on weight transformation to speed up the similarity computation. To improve the searching speed of similar blocks, we propose a two-stage searching algorithm based on a weight transformation. The method is able to reduce the searching time of the best matched block by examining key values for similarity detection. The experimental results show that the proposed algorithm can locate the forged region in forged images and performs well in terms of speed. In addition to the inpainting forgeries, our algorithm is also capable of detecting copy move forgeries. The rest of this paper is organized as follows. Section 2 summarizes the exemplar-based image inpainting technique. Section 3describes the proposed algorithm and the high-speed searching method. Section 4 illustrates the experimental results and analysis. Finally, we present our conclusions in Section 5.

2 Background knowledge

Image inpainting is a very active research field because it can effectively repair damaged or removed regions in a visually plausible way. Previously, pixel-based approaches were used to repair little blemishesor scratches, but this technique generates obvious blur when filling a larger region in the image. Criminisi's algorithm is the most popular exemplar-based inpainting algorithm among all the similar approaches.

In Criminisi's algorithm, an image is divided into target regions that are the regions to be inpainted and source regions which are regions to provide information to inpaint the target region. The goal of inpainting is to fill the target regions using information of source regions. An input image is divided into several overlapped patches, where the patches containing the partial area of the target regions are called target blocks and other blocks containing the source region only are called reference blocks.

2.1. The inpainting procedures are as follows

1. Compute inpainting priority among target blocks. The priority is judged by the data term and the confidence term. The data term shows the importance of the structure information carried by a block, and the confidence term determines whether the ratio of the available area of a target block is enough to be inpainted.
2. Select the target block with the highest priority and locate the reference block that contains the most similar color distribution to the target block.
3. Fill the target block's area to be inpainted using the reference block's corresponding area.
4. Update priorities among the target blocks.
5. Loop back to step 2 until the inpainted regions are entirely inpainted.

Fig. 1 shows a result produced by Ciminisi's algorithm. This figure suggests that Ciminisi's algorithm can eliminate the inpainting region and produce vivid forged results. Fig. 1(a) presents the original image in which there is a billboard and two dogs in the middle of the image. Fig. 1(b) gives the inpainted result using the Criminisi's algorithm, in which the billboard and the two dogs are completely removed.

Fig. 1. The image was forged by an exemplar-based inpainting technique (a) Original image (b) Forged image

..2. Proposed forgery detection algorithm

Our detection algorithm consists of two major modules: suspicious region detection and forged region detection. The first module searches for similar blocks in an image, selects candidates, and then groups them into several suspicious regions. The second part analyzes the multi-region relation of these suspicious regions and identifies the forged regions. Searching the most similar blocks is a time-consuming process. Instead of an exhaustive search, we propose a two-stage searching strategy, which has a comparable result to an exhaustive search but has higher speed.

..3. Suspicious region detection

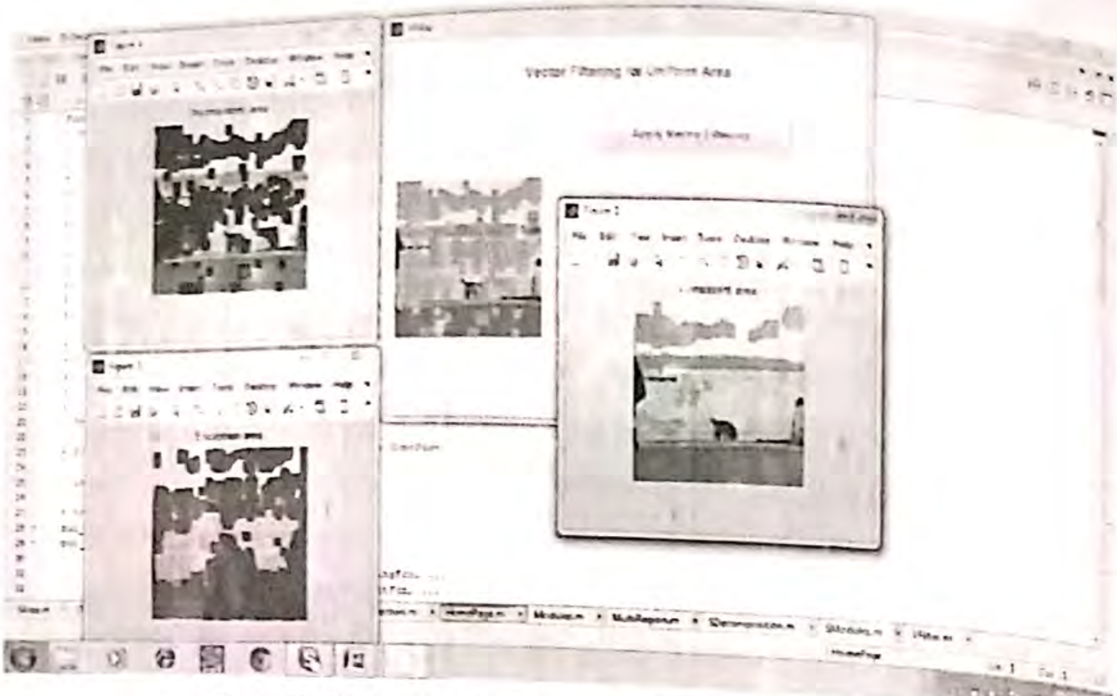
Because the forged regions are from the other parts of the same image, we apply the block similarity to detect the suspicious regions.

..3. Similar block computation

To locate similar blocks, we firstly divide an image into numbers of overlapped blocks and then compute similarity between every two blocks. Also, if this similarity is great enough, then these two blocks are identified as a similar pair, which indicates that the two blocks is highly possible to form a source/target relation in inpainting process. To determine the block similarity, we modified the similarity computation method to obtain better detection results. Assumes that there is an image with size of M×N, and the block size is R×R. Then the number of the overlapping blocks is (M−R+1)×(N−R+1).We define two kinds of blocks, target blocks (TB(x,y)) and reference blocks (RB(x,y)). Each block of an image is selected in turn to bẹ TB(x,y), and we search for all other blocks to find if there is similar.

..4. Vector filtering for uniform area

Uniform area is the major reason of the false alarm in forged region detection because these areas shares similar color distributions; hence blocks within this area tend to be recognized as similar blocks.



(Fig. 2) Vector filtering for Uniform area

For example, if an image (Fig. 2) contains a blue sky in the background, lots of similar blocks are detected in the uniform region . This image is not forged image; however, it produces many false positives. This section proposes a method to remove the false-alarmed blocks located at the uniform area with the characteristics of the similarity vectors. According to the similarity vector field, an image can be categorized into three kinds of areas: consistent area, inconsistent area and exception area. Each one contains different distribution of vector fields v(x, y). The followings are the definitions to the three kinds of areas:

(1) **Consistent area:** An area contains the similarity vectors with short length and unified directions. This phenomenon is resulted from the uniform color distributions in a uniform area, like picture of grasses and the sky. In a uniform area, a target block can always find a reference block which is very close to the target block. Thus, with the raster scan order, the detected similarity vectors in a uniform area are having short lengths and unified directions.

) **Inconsistent area**: An area contains the similarity vectors with long length and dispersed directions. This kind of areas is usually locating at the inpainted regions, which are constructed by neighboring the source regions.

) **Exception area**: An area doesn't have similarity vectors within it. These areas always occur at non-uniform backgrounds which own the texture distribution with high randomness.

Fig. 3 shows an example of the three types of areas. Fig. 3(a) is the iginal image and Fig.3(b) is the forged image. The dashed lines depict the iginal regions corresponding to the regions in the forged image. The light blue ea represents an inpainted area, at which the inconsistent area occurs. Since e light yellow area contains lots of uniformed textures, the lengths of the milarity vectors within the area will be very short. Therefore, the area will be lentified as the consistent areas. The light red area contains many randomized xtures, so it is hard to find an identical similarity vector using the zero-nnected path. According to the implementation of this work, the best cue to iscriminate an inconsistent area from the other types of areas is the length of he similarity vector rather than the direction of the vector.

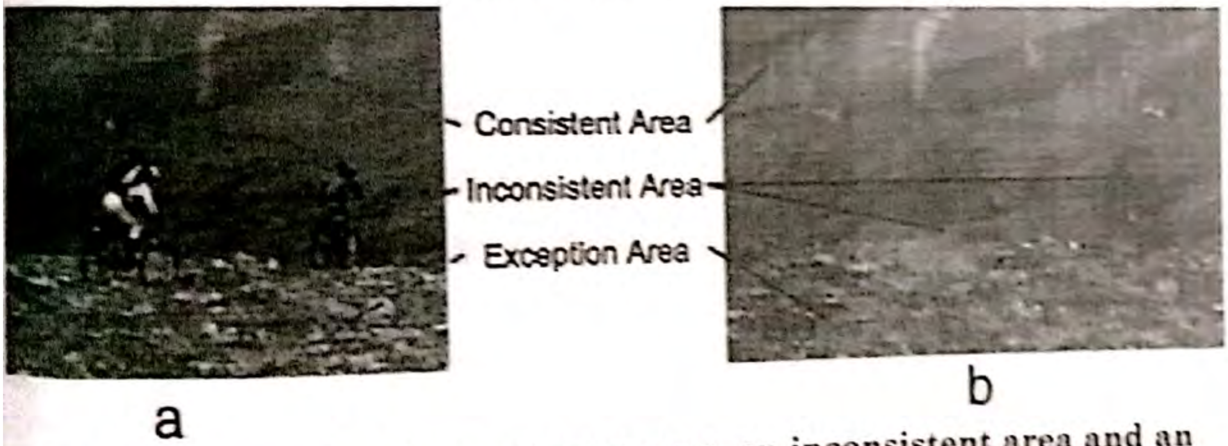


Fig. 3 An example of a consistent area, an inconsistent area and an exception area. (a) The original image (b) The forged image

Because the search follows the raster scan order, the detected similar blocks will be very close to each other; that is, the length of detected similarity vectors in a uniform region will be very short. This assumption is illustrated in

Figs. 4 and 5. Fig. 4shows an original image along with the corresponding target region and inpainted image, and Fig. 5gives comparison of the length of similarity vectors in the images in Fig. 4(a) and (c). It is not hard to find that false alarmed vectors of a uniform background have relative short length than that of a real inpainted region.

Fig. 4. The image was forged by exemplar-based inpainting technique. (a) Original image. (b) Selected Forged Region (c) Forged image. (The original image is sourced from Criminisi et al. [27])

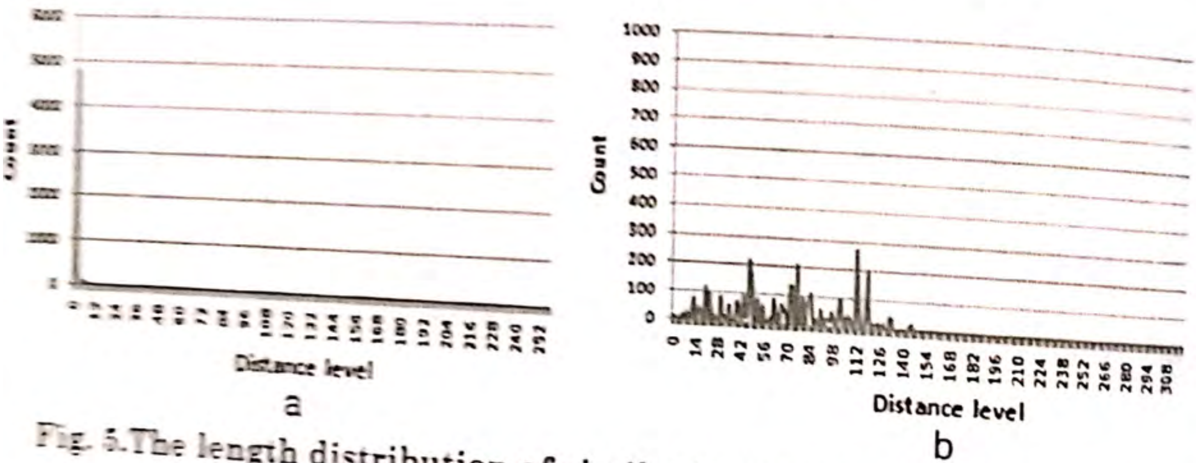


Fig. 5.The length distribution of similarity vectors. (a) The length distribution of Fig. 4(a). (b) The length distribution of Fig. 5(c).

5. Construction of suspicious region

A block (TB(x,y)) is defined as a suspicious block if SD(δTB(x,y))≥η and TB(x,y) belongs to an inconsistent area, where η is a threshold for the suspicious degree. According the definition of SD(δTB(x,y)), higher SD(δTB(x,y)) means the higher chance that a target block is a copy of a reference block. By taking account of the process of the exemplar based inpainting, the inpainting system may use a source block's partial content to fill a target block. If more than 50% area of a block is constructed by others, then the block is reasonable to be considered as a forged area. A reasonable choice of the value for η is 0.5.

2.6. Forged region detection

The identified suspicious regions still contain a few false positives, which come from the similar regions in background or noise interference. However, the inter-relations of these types of suspicious regions are not the same as the relation between the inpainting regions. This section presents a novel approach, multi-region relation, to filter out false positives and identify the forged region.

2.7. Multi-region relation among suspicious regions

A suspicious region is a collection of a number of suspicious blocks. Due to the process of block computation, a suspicious block in a suspicious region always comes along with another corresponding block in another region. Therefore, for a suspicious block within a suspicious region, the related suspicious block should be located at another suspicious region or the same region. When two suspicious regions contain a sufficient number of suspicious block pairs, the two regions are defined to have a region-link between them.

3. Result and Discussion

Experimental Results

This project is implemented using Matlab program where it is evaluated for recognize the tampered in digital image using Multi Region Relation technique. The performance of the algorithm is evaluated on several images. These pictures are the most widely used standard test images used for image forgery detection algorithms. For verifying the method used in this scheme, this project focused on in painting as well as copy move images. For performing experiment, this project took no of forged images from Google. One of them is shown in Fig

Figure.6 Experimental Images

This project took a number of images of both inpainting as well as copy move type. Fig.7, 8 shows how to load an image and then splitting them into number of overlapping blocks , similarity block computation.

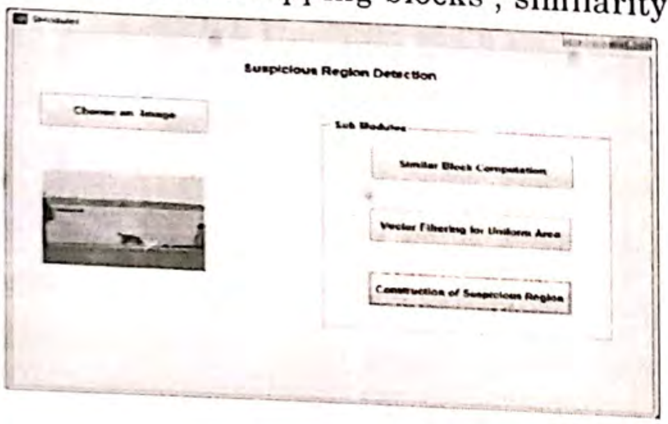


Fig. 7. Loading an image

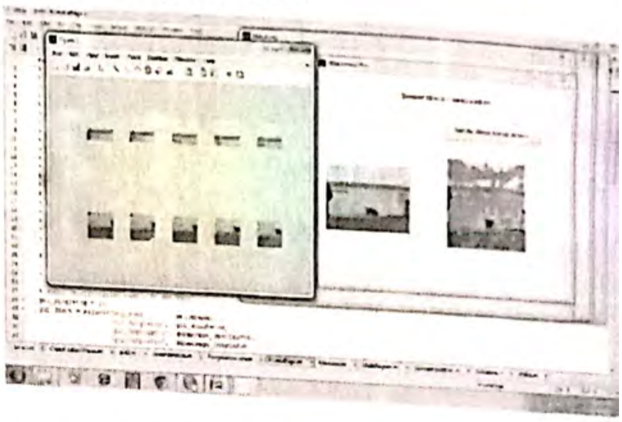


Fig 8. Similarity computation and block splitting

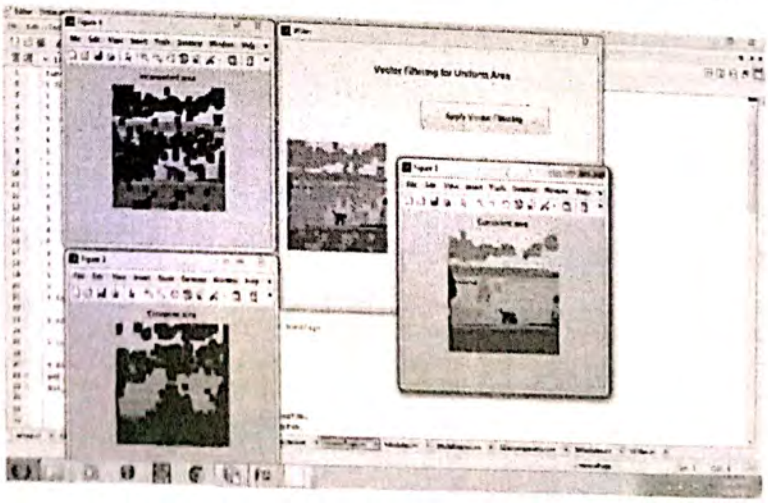


Fig 9. Vector Filtering

After the similarity block computation is over vector filtering should be e to remove false positives and also to classify the image into three area onsistent, exception area. Once vector filtering has been completed the next p is to construct the suspicious region. The inconsistent area has the high obability for being forged region because of high vector length. Fig.10. shows e construction of suspicious region.

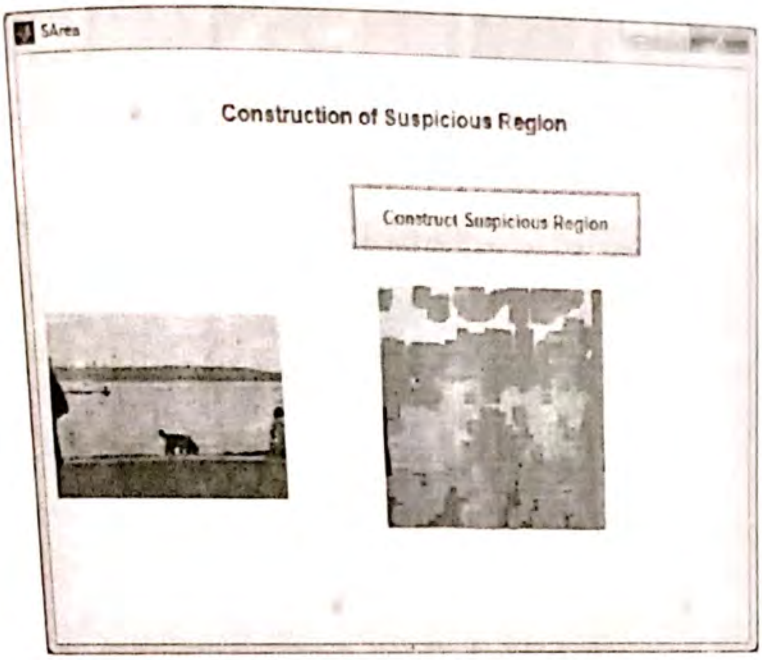


Fig .10 Construction of suspicious Region

Then taking the suspicious region as input Discrete cosine transform is applied on the suspicious region that has been constructed to detect the forged region. Fig 11.shows the detection of forged region.

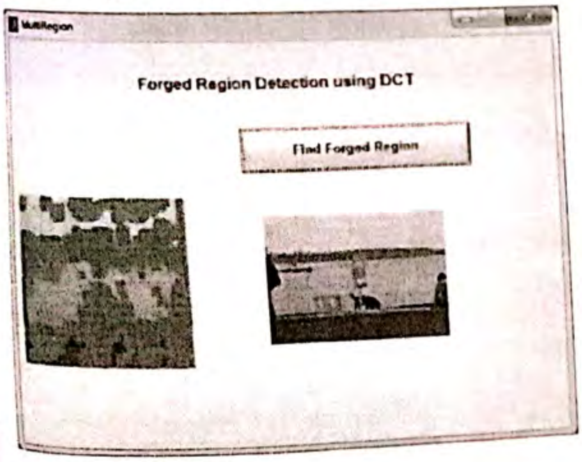


Fig 11. Finding forged regions using DCT

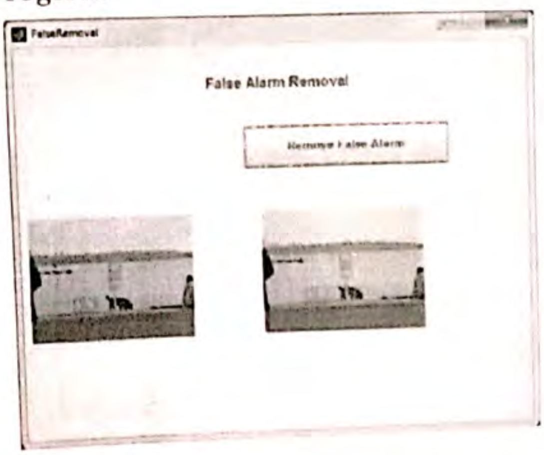


Fig 12. False Alarm Removal

From the above figure the forged region has been detected. It may have some gaps or false regions in order to remove that false alarm removal has to be done. Fig. 12 shows the final output image after false alarm removal.

Resultant Image

Original Image **Forged Image** **Output Image**

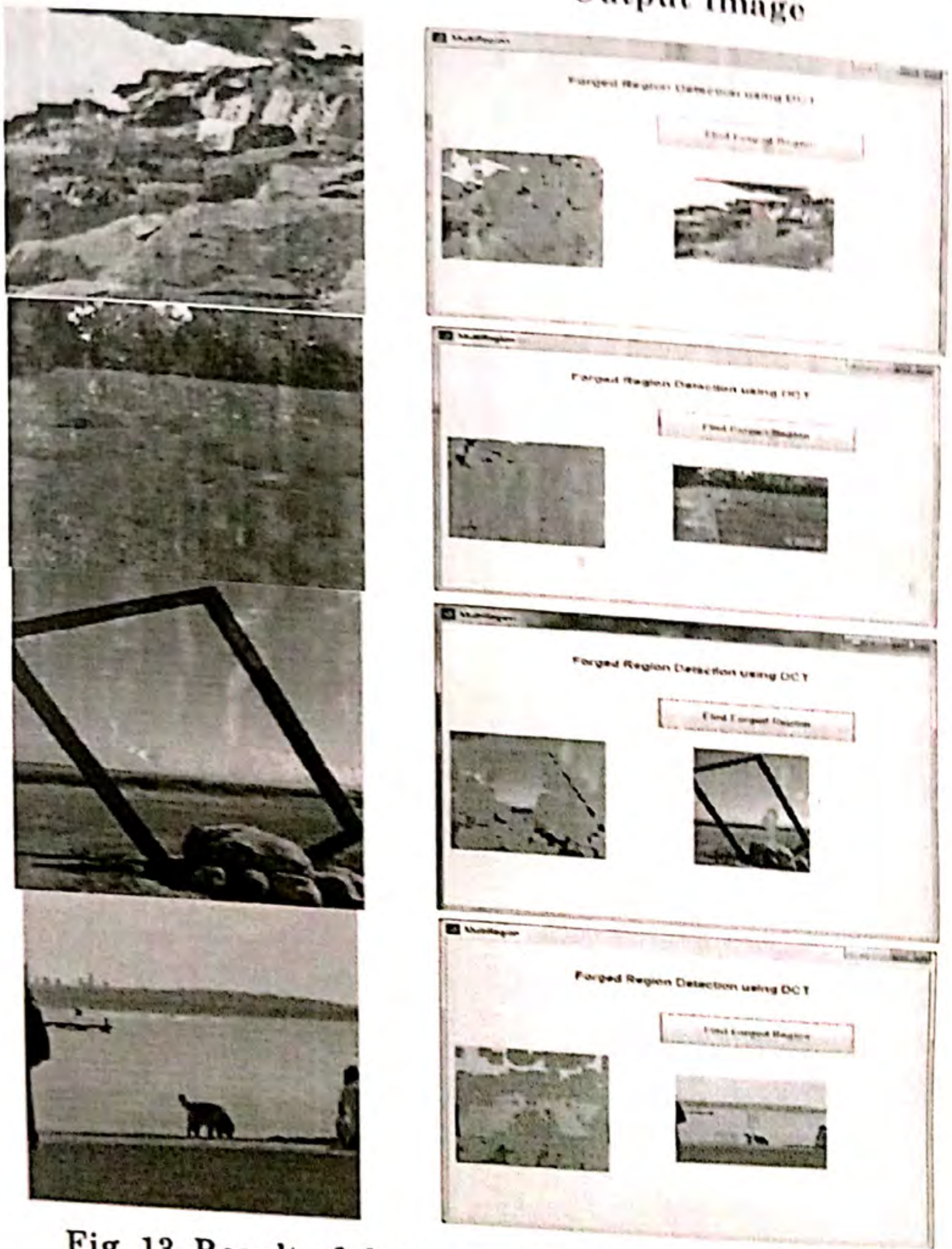


Fig. 13. Result of the inpainting image

The Fig. 13 show the original image and the forged image, output of the forged region using DCT.

4. Conclusion

In this paper, we propose a fast and effective forgery detection algorithm for exemplar-based inpainting forged image. We first search the suspicious regions using similar block computation, and then identify forged regions using the MRR technique. In addition to the inpainting type, our algorithm is also able to detect copy-move forgeries. Moreover, to speed up the execution time of similarity computation, we propose a fast searching algorithm based on weight transformation. The experimental results show that the proposed algorithm performs well with regards to both accuracy and speed while detecting forged regions in the inpainting forged image or copy-move forged image. There are still some limitations in this work. First, an assumption is that the forged region cannot be too small. Therefore, this system is incapable of locating forged regions of small sizes. Second, since the proposed method is based on locating similar parts within an image, we can only deal with the forged techniques such as copy move or inpainting techniques that copy verbatim patches from inside the image. If the forged region is further processed by some techniques like blurring, or the forged region is from different sources, the work may fail. In the future we will try to integrate some other techniques to solve these problems.

5. References

[1] H. Farid, Image forgery detection, IEEE Signal Process. Mag. (2009) 16-25.

[2] B. Mahdian, S. Saic, Blind methods for detecting image fakery, in: IEEE International Carnahan Conference on Security Technology, 2008, pp. 280–286.

[3] Z. Zhang, Y. Ren, X.J. Ping, Z.Y. He, S.Z. Zhang, A survey on passive-blind image forgery by doctor method detection, in: International Conference on Machine Learning and Cybernetics, 2008, pp. 3463–3467.

[4] W. Luo, Z. Qu, F. Pan, J. Huang, A survey of passive technology for digital image forensics, Front. Comput. Sci. (2007) 166–179.

[5] C. Rey, J.L. Dugelay, A survey of watermarking algorithms for image authentication, EURASIP J. Appl. Signal Process. (2002) 613–621 (special issue on image analysis for multimedia interactive services).